Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/017758

International filing date: 30 November 2004 (30.11.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2003-410784
Filing date: 09 December 2003 (09.12.2003)

Date of receipt at the International Bureau: 27 January 2005 (27.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/JP2004/017758

日本国特許庁
JAPAN PATENT OFFICE

02.12.20

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

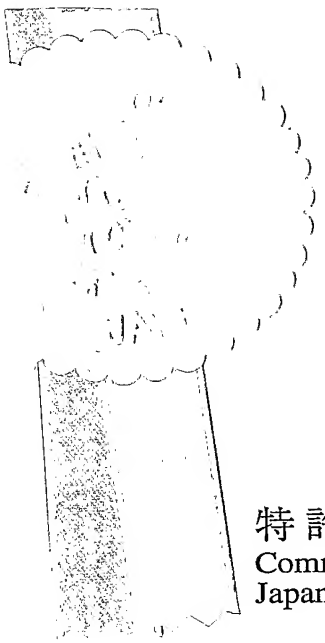
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１２月　９日

出願番号
Application Number: 特願２００３－４１０７８４

[ST. 10/C]: ［ＪＰ２００３－４１０７８４］

出願人
Applicant(s): 松下電器産業株式会社



２００５年　１月１４日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３１２２５８３

【書類名】　特許願
【整理番号】　2022550343
【提出日】　平成15年12月 9日
【あて先】　特許庁長官　殿
【国際特許分類】　G09L 1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　野仲　真佐男
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　館林　誠
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9003742

【書類名】特許請求の範囲
【請求項１】
可搬型の認証記録媒体と、前記認証記録媒体の正当性を認証する認証装置とからなる認証システムであって、
前記認証装置は、
前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段と、
チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成手段と、
前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力手段と、
レスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取手段と、
前記認証情報を用いて、受け取ったレスポンスデータに第１変換を施して認証データを生成し、生成した認証データと前記チャレンジデータとが一致するか否かを検証する検証手段と、
前記検証手段にて、一致すると検証した場合に、前記認証記録媒体が正当であると決定する決定手段とを備え、
前記認証記録媒体は、
耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段と、
前記認証装置より前記チャレンジデータを受け取るチャレンジデータ受取手段と、
前記証明情報を用いて、前記チャレンジデータに第２変換を施してレスポンスデータを生成するレスポンスデータ生成手段と、
生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力手段とを備え、
前記第１変換は前記第２変換の逆変換である
ことを特徴とする認証システム。
【請求項２】
可搬型の認証記録媒体の正当性を認証する認証装置であって、
前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段と、
チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成手段と、
前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力手段と、
前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取手段と、
受け取ったレスポンスデータと前記チャレンジデータと前記認証情報とを用いて、前記認証記録媒体の正当性を検証する検証手段と、
前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する決定手段と
を備えることを特徴とする認証装置。
【請求項３】
前記認証記録媒体は、宅配業者が有し、
前記認証装置は、前記宅配業者による訪問を受ける者が有し、
前記認証記録媒体は、宅配業者による訪問を示す第１訪問情報を記憶しており、
前記認証装置は、さらに、
宅配業者による訪問を示す第２訪問情報を記憶している訪問情報記憶手段と、
第１訪問情報を前記認証記録媒体より受け取り、受け取った第１訪問情報と前記第２訪問情報とが一致するか否かの判断を行う判断手段とを備え、
前記決定手段は、前記判断手段にて受け取った第１訪問情報と前記第２訪問情報とが一致すると判断した場合、及び前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する
ことを特徴とする請求項２に記載の認証装置。

【請求項４】
前記認証記録媒体は、暗号鍵を記憶しており、
前記認証情報は、前記暗号化鍵に対応する復号鍵であり、
前記レスポンスデータ受取手段は、前記暗号化鍵を用いて前記チャレンジデータを暗号化したレスポンスデータを受け取り、
前記検証手段は、前記レスポンスデータを、前記復号鍵を用いて復号して認証データを生成し、生成した認証データと前記データ生成手段にて記憶している前記チャレンジデータとが一致するか否かを検証する
ことを特徴とする請求項３に記載の認証装置。
【請求項５】
前記暗号化鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報であり、
前記認証装置は、さらに、
所有者証明情報に対応する、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を受け付ける受付手段を備え、
前記認証情報記憶手段は、受け付けた所有者認証情報を記憶し、
前記レスポンスデータ受取手段は、前記所有者証明情報を用いて前記チャレンジデータを暗号化したレスポンスデータを受け取り、
前記検証手段は、前記レスポンスデータを、前記所有者認証情報を用いて復号して認証データを生成する
ことを特徴とする請求項４に記載の認証装置。
【請求項６】
前記認証情報は、秘密鍵であり、
前記認証記録媒体は、前記秘密鍵と同一の秘密鍵を記憶しており、
前記レスポンスデータ受取手段は、秘密鍵暗号により前記チャレンジデータを暗号化したレスポンスデータを前記認証記録媒体より受け取り、
前記検証手段は、前記チャレンジデータを、前記秘密鍵を用いた秘密鍵暗号により暗号化して暗号化認証データを生成し、生成した暗号化認証データと、受け取ったレスポンスデータとが一致するか否かを検証する
ことを特徴とする請求項３に記載の認証装置。
【請求項７】
前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報であり、
前記認証装置は、さらに、
所有者認証情報を受け付ける受付手段を備え、
前記認証情報記憶手段は、受け付けた所有者認証情報を記憶し、
前記検証手段は、前記チャレンジデータを、前記所有者認証情報を用いて暗号化して暗号化認証データを生成する
ことを特徴とする請求項６に記載の認証装置。
【請求項８】
前記認証記録媒体は、秘密鍵を記憶しており、
前記認証情報は、前記秘密鍵に対応する公開鍵であり、
前記レスポンスデータ受取手段は、前記秘密鍵を用いて前記チャレンジデータの電子署名であるレスポンスデータを受け取り、
前記検証手段は、受け取ったレスポンスデータと前記公開鍵と前記チャレンジデータとを用いて署名検証する
ことを特徴とする請求項３に記載の認証装置。
【請求項９】
前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応しており、

前記認証装置は、さらに、
所有者証明情報に対応する、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を受け付ける受付手段を備え、
前記認証情報記憶手段は、前記認証情報を記憶する代わりに、受け付けた所有者認証情報を記憶し、
前記検証手段は、前記所有者認証情報から前記秘密鍵に対応する公開鍵を生成し、生成した公開鍵と前記チャレンジデータと前記レスポンスデータとを用いて署名検証する
ことを特徴とする請求項８に記載の認証装置。
【請求項１０】
前記認証装置は、さらに、
宅配業者による訪問の正当性を検証するための訪問検証情報を記憶している検証情報記憶手段と、
訪問検証チャレンジデータを生成し、生成した訪問検証チャレンジデータを記憶する訪問検証データ生成手段と、
前記訪問検証チャレンジデータを前記認証記録媒体へ出力する訪問検証チャレンジデータ出力手段と、
前記訪問検証チャレンジデータより生成された訪問検証レスポンスデータを前記認証記録媒体より受け取る訪問検証レスポンスデータ受取手段と、
受け取った訪問検証レスポンスデータと、前記訪問検証情報と前記訪問検証チャレンジデータとを用いて、宅配業者による訪問の正当性を検証する訪問検証手段とを備え、
前記決定手段は、前記判断手段にて受け取った第１訪問情報と前記第２訪問情報とが一致すると判断した場合、前記訪問検証手段にて肯定的に検証した場合、及び前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する
ことを特徴とする請求項３に記載の認証装置。
【請求項１１】
前記認証装置は、さらに、
認証情報を配信する配信装置とネットワークを介して接続されており、
前記認証装置は、さらに、
前記配信装置より配信される認証情報を受信する受信手段と、
前記認証情報を前記認証情報記憶手段に書き込む書込手段と
を備えることを特徴とする請求項３に記載の認証装置。
【請求項１２】
前記チャレンジデータ出力手段は、前記チャレンジデータを出力する代わりに、前記チャレンジデータから変換チャレンジ情報を生成し、生成した変換チャレンジ情報を前記認証記録媒体へ出力する
ことを特徴とする請求項３に記載の認証装置。
【請求項１３】
前記変換チャレンジ情報は、光信号、バーコード、ＱＲコード、赤外線信号、及び音声信号のうち何れかからなる情報である
ことを特徴とする請求項１２に記載の認証装置。
【請求項１４】
前記レスポンスデータ受取手段は、前記レスポンスデータを受け取る代わりに、前記レスポンスデータより生成された変換レスポンス情報を受け取り、受け取った変換レスポンス情報より前記レスポンスデータを生成する
ことを特徴とする請求項３に記載の認証装置。
【請求項１５】
前記変換レスポンス情報は、光信号、バーコード、ＱＲコード、赤外線信号、及び音声信号のうち何れかからなる情報である
ことを特徴とする請求項１４に記載の認証装置。
【請求項１６】

前記認証装置は、さらに、
自己を識別する装置識別子を記憶している識別子記憶手段と、
前記決定手段にて、前記認証記録媒体が正当であると決定した場合に、前記装置識別子を前記認証記録媒体へ出力する識別子出力手段とを
備えることを特徴とする請求項３に記載の認証装置。
【請求項１７】
前記認証装置は、携帯電話機である
ことを特徴とする請求項２乃至１６に記載の認証装置。
【請求項１８】
可搬型の認証記録媒体の正当性を認証する認証装置であって、
チャレンジデータを生成するための認証情報を記憶している認証情報記憶手段と、
第１データを生成し、生成した第１データを記憶するデータ生成手段と、
前記認証情報を用いて、前記第１データを変換して、チャレンジデータを生成する変換手段と、
生成したチャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力手段と、
前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取手段と、
受け取ったレスポンスデータと前記第１データとが一致するか否かを検証する検証手段と、
前記検証手段にて、一致すると検証した場合に、前記認証記録媒体が正当であると決定する決定手段と
を備えることを特徴とする認証装置。
【請求項１９】
前記認証記録媒体は、宅配業者にて所有され、
前記認証装置は、前記宅配業者による訪問を受ける者が有し、
前記認証記録媒体は、前記宅配業者による訪問を示す第１訪問情報を記憶しており、
前記認証装置は、さらに、
前記宅配業者による訪問を示す第２訪問情報を記憶している訪問情報記憶手段と、
第１訪問情報を前記認証記録媒体より受け取り、受け取った第１訪問情報と前記第２訪問情報とが一致するか否かの判断を行う判断手段とを備え、
前記決定手段は、前記判断手段にて受け取った第１訪問情報と前記第２訪問情報とが一致すると判断した場合、及び前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する
ことを特徴とする請求項１８に記載の認証装置。
【請求項２０】
前記認証記録媒体は、秘密鍵を記憶しており、
前記認証情報は、前記秘密鍵に対応する公開鍵であり、
前記変換手段は、前記公開鍵を用いて、前記第１データを暗号化してチャレンジデータを生成し、
前記レスポンスデータ受取手段は、前記秘密鍵を用いて前記チャレンジデータを復号したレスポンスデータを受け取る
ことを特徴とする請求項１９に記載の認証装置。
【請求項２１】
前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応しており、
前記認証装置は、さらに、
所有者証明情報に対応する、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を受け付ける受付手段を備え、
前記認証情報記憶手段は、前記認証情報を記憶する代わりに、受け付けた所有者認証情

報を記憶し、
　前記変換手段は、記憶している所有者認証情報を用いて前記暗号化鍵に対応する公開鍵を生成し、生成した公開鍵を用いて前記第１データを暗号化してチャレンジデータを生成する
　ことを特徴とする請求項２０に記載の認証装置。
【請求項２２】
　認証装置により認証がなされる可搬型の認証記録媒体であって、
　耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段と、
　前記認証装置よりチャレンジデータを受け取るチャレンジデータ受取手段と、
　前記証明情報を用いて前記チャレンジデータからレスポンスデータを生成するレスポンスデータ生成手段と、
　生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力手段と
　を備えることを特徴とする認証記録媒体。
【請求項２３】
　前記認証記録媒体は、宅配業者が有し、
　前記認証記録媒体は、さらに、
　宅配業者による訪問を示す訪問情報を記憶している訪問情報記憶手段と、
　前記訪問情報を前記認証装置へ出力する訪問情報出力手段と
　を備えることを特徴とする請求項２２に記載の認証記録媒体。
【請求項２４】
　前記証明情報は、暗号化鍵であり、
　前記レスポンスデータ生成手段は、前記暗号化鍵を用いて前記チャレンジデータを暗号して、レスポンスデータを生成する
　ことを特徴とする請求項２３に記載の認証記録媒体。
【請求項２５】
　前記暗号化鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報であり、
　前記レスポンスデータ生成手段は、前記所有者証明情報を用いて、前記チャレンジデータを暗号化して、レスポンスデータを生成する
　ことを特徴とする請求項２４に記載の認証記録媒体。
【請求項２６】
　前記認証情報は、秘密鍵であり、
　前記チャレンジデータは、前記秘密鍵に対応する公開鍵を用いて、前記認証装置により生成されたデータが暗号化されたデータであり、
　前記レスポンスデータ生成手段は、前記秘密鍵を用いて受け取ったチャレンジデータを復号して、レスポンスデータを生成する
　ことを特徴とする請求項２３に記載の認証記録媒体。
【請求項２７】
　前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応した鍵であり、
　前記公開鍵は、前記所有者証明情報に対応する前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を用いて前記認証記録媒体にて生成された鍵である
　ことを特徴とする請求項２６に記載の認証記録媒体。
【請求項２８】
　前記認証情報は、秘密鍵であり、
　前記レスポンスデータ生成手段は、前記秘密鍵を用いて受け取ったチャレンジデータの電子署名であるレスポンスデータを生成する
　ことを特徴とする請求項２３に記載の認証記録媒体。
【請求項２９】

前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応した鍵である
ことを特徴とする請求項２８に記載の認証記録媒体。
【請求項３０】
前記チャレンジデータ受取手段は、前記チャレンジデータを受け取る代わりに、前記チャレンジデータから生成された変換チャレンジ情報を受け取り、受け取った変換チャレンジ情報より前記チャレンジデータを生成する
ことを特徴とする請求項２３に記載の認証記録媒体。
【請求項３１】
前記変換チャレンジ情報は、光信号、バーコード、ＱＲコード、赤外線信号、及び音声信号のうち何れかからなる情報である
ことを特徴とする請求項３０に記載の認証記録媒体。
【請求項３２】
前記レスポンスデータ出力手段は、前記レスポンスデータを出力する代わりに、前記レスポンスデータから変換レスポンス情報を生成し、生成した変換レスポンス情報を出力する
ことを特徴とする請求項２３に記載の認証記録媒体。
【請求項３３】
前記変換レスポンス情報は、光信号、バーコード、ＱＲコード、赤外線信号、及び音声信号のうち何れかからなる情報である
ことを特徴とする請求項３２に記載の認証記録媒体。
【請求項３４】
前記認証記録媒体は、さらに、
前記認証装置より、前記認証装置を識別する装置識別子を受け取る識別子受取手段と、
受け取った装置識別子を記憶する識別子記憶手段とを
備えることを特徴とする請求項２３に記載の認証記録媒体。
【請求項３５】
可搬型の認証記録媒体の正当性を認証する認証装置に用いられる認証方法であって、
前記認証装置は、
前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段を備え、
前記認証方法は、
チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成ステップと、
前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力ステップと、
前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取ステップと、
受け取ったレスポンスデータと前記チャレンジデータと前記認証情報とを用いて、前記認証記録媒体の正当性を検証する検証ステップと、
前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する決定ステップと
を含むことを特徴とする認証方法。
【請求項３６】
可搬型の認証記録媒体の正当性を認証する認証装置に用いられる認証プログラムであって、
前記認証装置は、
前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段を備え、
前記認証プログラムは、

チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成ステップと、
前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力ステップと、
前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取ステップと、
受け取ったレスポンスデータと前記チャレンジデータと前記認証情報とを用いて、前記認証記録媒体の正当性を検証する検証ステップと、
前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する決定ステップと
を含むことを特徴とする認証プログラム。
【請求項３７】
可搬型の認証記録媒体の正当性を認証する認証装置に用いられる認証プログラムを記録しているコンピュータ読み取り可能な認証プログラム記録媒体であって、
前記認証装置は、
前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段を備え、
前記認証プログラムは、
チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成ステップと、
前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力ステップと、
前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取ステップと、
受け取ったレスポンスデータと前記チャレンジデータと前記認証情報とを用いて、前記認証記録媒体の正当性を検証する検証ステップと、
前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する決定ステップと
を含むことを特徴とする認証プログラム記録媒体。
【請求項３８】
認証装置により認証がなされる可搬型の認証記録媒体に用いられる証明方法であって、
前記認証記録媒体は、
耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段を備え、
前記証明方法は、
前記認証装置よりチャレンジデータを受け取るチャレンジデータ受取ステップと、
前記証明情報を用いて前記チャレンジデータからレスポンスデータを生成するレスポンスデータ生成ステップと、
生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力ステップと
を含むことを特徴とする証明方法。
【請求項３９】
認証装置により認証がなされる可搬型の認証記録媒体に用いられる証明プログラムであって、
前記認証記録媒体は、
耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段を備え、
前記証明プログラムは、
前記認証装置よりチャレンジデータを受け取るチャレンジデータ受取ステップと、
前記証明情報を用いて前記チャレンジデータからレスポンスデータを生成するレスポンスデータ生成ステップと、

生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力ステップとを含むことを特徴とする証明プログラム。

【請求項４０】

認証装置により認証がなされる可搬型の認証記録媒体に用いられる証明プログラムを記録しているコンピュータ読み取り可能な証明プログラム記録媒体であって、

前記認証記録媒体は、

耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段を備え、

前記証明プログラムは、

前記認証装置よりチャレンジデータを受け取るチャレンジデータ受取ステップと、

前記証明情報を用いて前記チャレンジデータからレスポンスデータを生成するレスポンスデータ生成ステップと、

生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力ステップとを含むことを特徴とする証明プログラム記録媒体。

【書類名】明細書
【発明の名称】認証システム
【技術分野】
【０００１】
本発明は、記録媒体の所有者の身元を認証する技術に関する。
【背景技術】
【０００２】
従来、宅内にいる者が、訪問者の身元をインターホンやテレビドアホンなどを利用して確認する方法が一般的に用いられている。
しかしながら、上記の方法では、訪問者が容姿や声を偽ることによって、宅内にいる者を欺くことができるため、宅内にいる者が、訪問者の身元を確実に確認することは困難である。
【０００３】
そこで、特許文献１に示すような個人情報表示システムが開示されている。この個人情報表示システムは、個人情報及び個人特定情報を予め記憶しているサーバと、個人特定情報を通信回線を介してサーバに送信するユーザ端末とを有し、サーバは、予め記憶している個人特定情報とユーザ端末から送信された個人特定情報とを照合し、照合結果に応じて、個人特定情報と関連付けられて記憶している個人情報をユーザ端末に送信し、ユーザ端末は、サーバから受信した個人情報を表示する。この個人情報表示システムによって、宅配業者等の訪問者の身分を確実に確認することが可能になる。
【特許文献１】特開２００３－１０８５２９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、上記に示す個人情報表示システムに限らず様々な形態にて訪問者の確認を行うシステムの要望がある。
そこで、本発明は、従来技術とは異なる、訪問者の身元の認証を行うことのできる認証システム、認証装置、認証記録媒体、認証方法、認証プログラム、認証プログラム記録媒体、証明方法、証明プログラム及び証明プログラム記録媒体を提供することを目的とする。
【課題を解決するための手段】
【０００５】
上記目的を達成するために、本発明は、可搬型の認証記録媒体と、前記認証記録媒体の正当性を認証する認証装置とからなる認証システムであって、前記認証装置は、前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段と、チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成手段と、前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力手段と、レスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取手段と、前記認証情報を用いて、受け取ったレスポンスデータに第１変換を施して認証データを生成し、生成した認証データと前記チャレンジデータとが一致するか否かを検証する検証手段と、前記検証手段にて、一致すると検証した場合に、前記認証記録媒体が正当であると決定する決定手段とを備え、前記認証記録媒体は、耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段と、前記認証装置より前記チャレンジデータを受け取るチャレンジデータ受取手段と、前記証明情報を用いて、前記チャレンジデータに第２変換を施してレスポンスデータを生成するレスポンスデータ生成手段と、生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力手段とを備え、前記第１変換は前記第２変換の逆変換であることを特徴とする。
【発明の効果】
【０００６】
課題を解決するための手段に示した構成によると、認証システムは、認証記録媒体の正

当性を検証する場合に、レスポンスデータを受け取った認証装置にて行う。このとき、レスポンスデータを生成する際に用いる証明情報は、耐タンパ性を有する証明情報記憶手段にて記憶されているため、第三者にて改竄されることはない。そのため、認証記録媒体が正当であると決定された場合には、認証記録媒体の所有者を正当な所有者であると決定することができる。

【０００７】

また、本発明は、可搬型の認証記録媒体の正当性を認証する認証装置であって、前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段と、チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成手段と、前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力手段と、前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取手段と、受け取ったレスポンスデータと前記チャレンジデータと前記認証情報とを用いて、前記認証記録媒体の正当性を検証する検証手段と、前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する決定手段とを備えることを特徴とする。

【０００８】

この構成によると、認証装置は、当該認証装置にて記憶しているチャレンジデータと認証情報と認証記録媒体より受け取ったレスポンスデータとを用いて、認証記録媒体の正当性を検証する。これにより、認証記録媒体が正当であると決定された場合には、認証記録媒体の所有者を正当な所有者であると決定することができる。

ここで、前記認証記録媒体は、宅配業者が有し、前記認証装置は、前記宅配業者による訪問を受ける者が有し、前記認証記録媒体は、宅配業者による訪問を示す第１訪問情報を記憶しており、前記認証装置は、さらに、宅配業者による訪問を示す第２訪問情報を記憶している訪問情報記憶手段と、第１訪問情報を前記認証記録媒体より受け取り、受け取った第１訪問情報と前記第２訪問情報とが一致するか否かの判断を行う判断手段とを備え、前記決定手段は、前記判断手段にて受け取った第１訪問情報と前記第２訪問情報とが一致すると判断した場合、及び前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定するとしてもよい。

【０００９】

この構成によると、認証装置は、さらに、第１訪問情報と第２訪問情報とが一致するか否かを判断を行い、認証記録媒体が正当であることを決定するための条件が、さらに付加されていることにより、認証記録媒体の正当性がより確かなものとなる。つまり、認証記録媒体の所有者の正当性がより確かなものとなるため、宅配業者による訪問が確かな訪問であると決定することができる。

【００１０】

ここで、前記認証記録媒体は、暗号鍵を記憶しており、前記認証情報は、前記暗号化鍵に対応する復号鍵であり、前記レスポンスデータ受取手段は、前記暗号化鍵を用いて前記チャレンジデータを暗号化したレスポンスデータを受け取り、前記検証手段は、前記レスポンスデータを、前記復号鍵を用いて復号して認証データを生成し、生成した認証データと前記データ生成手段にて記憶している前記チャレンジデータとが一致するか否かを検証するとしてもよい。

【００１１】

この構成によると、認証装置は、チャレンジデータが認証記録媒体が記憶している暗号鍵にて暗号化されたレスポンスデータを、前記暗号鍵に対応する復号鍵を用いて、復号して、認証データを生成し、生成した認証データとチャレンジデータとが一致するか否かを検証することができる。つまり、認証装置は、暗号処理を利用して、認証記録媒体の認証を行うことができる。

【００１２】

ここで、前記暗号化鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報であり、前記認証装置は、さらに、所有者証明情報に対応する、前記認証記録媒体

の所有者の生体科学的特徴を示す所有者認証情報を受け付ける受付手段を備え、前記認証情報記憶手段は、受け付けた所有者認証情報を記憶し、前記レスポンスデータ受取手段は、前記所有者証明情報を用いて前記チャレンジデータを暗号化したレスポンスデータを受け取り、前記検証手段は、前記レスポンスデータを、前記所有者認証情報を用いて復号して認証データを生成するとしてもよい。

【００１３】

この構成によると、認証装置は、認証記録媒体の所有者の生体科学的特徴を示す情報を用いて、レスポンスデータを復号して認証データを生成することができる。

ここで、前記認証情報は、秘密鍵であり、前記認証記録媒体は、前記秘密鍵と同一の秘密鍵を記憶しており、前記レスポンスデータ受取手段は、秘密鍵暗号により前記チャレンジデータを暗号化したレスポンスデータを前記認証記録媒体より受け取り、前記検証手段は、前記チャレンジデータを、前記秘密鍵を用いた秘密鍵暗号により暗号化して暗号化認証データを生成し、生成した暗号化認証データと、受け取ったレスポンスデータとが一致するか否かを検証するとしてもよい。

【００１４】

この構成によると、認証装置は、チャレンジデータが認証記録媒体にて記憶している秘密鍵を用いた秘密鍵暗号により暗号化されたレスポンスデータと、チャレンジデータが当該認証装置が記憶している前記秘密鍵と同一の秘密鍵を用いた秘密鍵暗号により暗号化された暗号化認証データとを用いて、認証記録媒体の正当性を検証することができる。

ここで、前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報であり、前記認証装置は、さらに、所有者認証情報を受け付ける受付手段を備え、前記認証情報記憶手段は、受け付けた所有者認証情報を記憶し、前記検証手段は、前記チャレンジデータを、前記所有者認証情報を用いて暗号化して暗号化認証データを生成するとしてもよい。

【００１５】

この構成によると、認証装置は、認証記録媒体の所有者の生体科学的特徴を示す情報を用いて、チャレンジデータを暗号化して暗号化認証データを生成することができる。

ここで、前記認証記録媒体は、秘密鍵を記憶しており、前記認証情報は、前記秘密鍵に対応する公開鍵であり、前記レスポンスデータ受取手段は、前記秘密鍵を用いて前記チャレンジデータの電子署名であるレスポンスデータを受け取り、前記検証手段は、受け取ったレスポンスデータと前記公開鍵と前記チャレンジデータとを用いて署名検証するとしてもよい。

【００１６】

この構成によると、認証装置は、チャレンジデータの電子署名であるレスポンスデータを受け取り、チャレンジデータと、公開鍵と、受け取ったレスポンスデータと用いて署名検証を行うことにより、認証記録媒体の正当性を検証することができる。

ここで、前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応しており、前記認証装置は、さらに、

所有者証明情報に対応する、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を受け付ける受付手段を備え、前記認証情報記憶手段は、前記認証情報を記憶する代わりに、受け付けた所有者認証情報を記憶し、前記検証手段は、前記所有者認証情報から前記秘密鍵に対応する公開鍵を生成し、生成した公開鍵と前記チャレンジデータと前記レスポンスデータとを用いて署名検証するとしてもよい。

【００１７】

この構成によると、認証装置は、認証記録媒体の所有者の生体科学的特徴を示す情報と、チャレンジデータと、レスポンスデータとを用いて、署名検証することができる。

ここで、前記認証装置は、さらに、宅配業者による訪問の正当性を検証するための訪問検証情報を記憶している検証情報記憶手段と、訪問検証チャレンジデータを生成し、生成した訪問検証チャレンジデータを記憶する訪問検証データ生成手段と、前記訪問検証チャレンジデータを前記認証記録媒体へ出力する訪問検証チャレンジデータ出力手段と、前記

訪問検証チャレンジデータより生成された訪問検証レスポンスデータを前記認証記録媒体より受け取る訪問検証レスポンスデータ受取手段と、受け取った訪問検証レスポンスデータと、前記訪問検証情報と前記訪問検証チャレンジデータとを用いて、宅配業者による訪問の正当性を検証する訪問検証手段とを備え、前記決定手段は、前記判断手段にて受け取った第１訪問情報と前記第２訪問情報とが一致すると判断した場合、前記訪問検証手段にて肯定的に検証した場合、及び前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定するとしてもよい。

【００１８】

この構成によると、宅配業者による訪問の正当性の検証を行い、認証記録媒体が正当であることを決定するための条件が、さらに付加されていることにより、認証記録媒体の正当性がより確かなものとなる。つまり、宅配業者による訪問がより確かな訪問であると決定することができる。

ここで、前記認証装置は、さらに、認証情報を配信する配信装置とネットワークを介して接続されており、前記認証装置は、さらに、前記配信装置より配信される認証情報を受信する受信手段と、前記認証情報を前記認証情報記憶手段に書き込む書込手段とを備えるとしてもよい。

【００１９】

この構成によると、認証装置は、配信装置より認証情報を受信し、受信した認証情報を認証情報記憶手段へ書き込むことができる。これにより、宅配業者は、訪問する前に、事前に配信装置を用いて、訪問時の認証に必要な認証情報を配信することができ、認証装置は、宅配業者による訪問を受けた際に行う認証に必要な認証情報のみを、事前に受信することができる。

【００２０】

ここで、前記チャレンジデータ出力手段は、前記チャレンジデータを出力する代わりに、前記チャレンジデータから変換チャレンジ情報を生成し、生成した変換チャレンジ情報を前記認証記録媒体へ出力するとしてもよい。

この構成によると、認証装置は、チャレンジデータの代わりに、チャレンジデータより生成した変換チャレンジ情報を認証記録媒体へ出力することができる。

【００２１】

ここで、前記変換チャレンジ情報は、光信号、バーコード、ＱＲコード、赤外線信号、及び音声信号のうち何れかからなる情報であるとしてもよい。

この構成によると、認証装置は、光信号、バーコード、ＱＲコード、赤外線信号、及び音声信号のうち何れかからなる変換チャレンジ情報を、認証記録媒体へ出力することができる。

【００２２】

ここで、前記レスポンスデータ受取手段は、前記レスポンスデータを受け取る代わりに、前記レスポンスデータより生成された変換レスポンス情報を受け取り、受け取った変換レスポンス情報より前記レスポンスデータを生成するとしてもよい。

この構成によると、認証装置は、レスポンスデータの代わりに、レスポンスデータより生成された変換レスポンス情報を認証記録媒体より受け取り、受け取った変換レスポンス情報よりレスポンスデータを生成することができる。

【００２３】

ここで、前記変換レスポンス情報は、光信号、バーコード、ＱＲコード、赤外線信号、及び音声信号のうち何れかからなる情報であるとしてもよい。

この構成によると、認証装置は、光信号、バーコード、ＱＲコード、赤外線信号、及び音声信号のうち何れかからなる変換レスポンス情報を、認証記録媒体より受け取り、受け取った変換レスポンス情報よりレスポンスデータを生成することができる。

【００２４】

ここで、前記認証装置は、さらに、自己を識別する装置識別子を記憶している識別子記憶手段と、前記決定手段にて、前記認証記録媒体が正当であると決定した場合に、前記装

置識別子を前記認証記録媒体へ出力する識別子出力手段とを備えるとしてもよい。

この構成によると、認証装置は、認証記録媒体が正当であると決定した場合に、装置識別子を認証記録媒体へ出力することができる。

【００２５】

また、本発明は、可搬型の認証記録媒体の正当性を認証する認証装置であって、チャレンジデータを生成するための認証情報を記憶している認証情報記憶手段と、第１データを生成し、生成した第１データを記憶するデータ生成手段と、前記認証情報を用いて、前記第１データを変換して、チャレンジデータを生成する変換手段と、生成したチャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力手段と、前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取手段と、受け取ったレスポンスデータと前記第１データとが一致するか否かを検証する検証手段と、前記検証手段にて、一致すると検証した場合に、前記認証記録媒体が正当であると決定する決定手段とを備えることを特徴とする。

【００２６】

この構成によると、認証装置は、当該認証装置にて記憶している第１データと認証情報と認証記録媒体より受け取ったレスポンスデータとを用いて、認証記録媒体の正当性を検証する。これにより、認証記録媒体が正当であると決定された場合には、認証記録媒体の所有者を正当な所有者であると決定することができる。

ここで、前記認証記録媒体は、宅配業者にて所有され、前記認証装置は、前記宅配業者による訪問を受ける者が有し、前記認証記録媒体は、前記宅配業者による訪問を示す第１訪問情報を記憶しており、前記認証装置は、さらに、前記宅配業者による訪問を示す第２訪問情報を記憶している訪問情報記憶手段と、第１訪問情報を前記認証記録媒体より受け取り、受け取った第１訪問情報と前記第２訪問情報とが一致するか否かの判断を行う判断手段とを備え、前記決定手段は、前記判断手段にて受け取った第１訪問情報と前記第２訪問情報とが一致すると判断した場合、及び前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定するとしてもよい。

【００２７】

この構成によると、認証装置は、さらに、第１訪問情報と第２訪問情報とが一致するか否かを判断を行い、認証記録媒体が正当であることを決定するための条件が、さらに付加されていることにより、認証記録媒体の正当性がより確かなものとなる。つまり、認証記録媒体の所有者の正当性がより確かなものとなるため、宅配業者による訪問が確かな訪問であると決定することができる。

【００２８】

ここで、前記認証記録媒体は、秘密鍵を記憶しており、前記認証情報は、前記秘密鍵に対応する公開鍵であり、前記変換手段は、前記公開鍵を用いて、前記第１データを暗号化してチャレンジデータを生成し、前記レスポンスデータ受取手段は、前記秘密鍵を用いて前記チャレンジデータを復号したレスポンスデータを受け取るとしてもよい。

この構成によると、認証装置は、公開鍵暗号を用いて、認証記録媒体の正当性を検証することができる。

【００２９】

ここで、前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応しており、前記認証装置は、さらに、所有者証明情報に対応する、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を受け付ける受付手段を備え、前記認証情報記憶手段は、前記認証情報を記憶する代わりに、受け付けた所有者認証情報を記憶し、前記変換手段は、記憶している所有者認証情報を用いて前記暗号化鍵に対応する公開鍵を生成し、生成した公開鍵を用いて前記第１データを暗号化してチャレンジデータを生成するとしてもよい。

【００３０】

この構成によると、認証装置は、認証記録媒体の所有者の生体科学的特徴を示す情報に対応する公開鍵を生成し、生成した公開鍵を用いて、チャレンジデータを生成することが

できる。

また、本発明は、認証装置により認証がなされる可搬型の認証記録媒体であって、耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段と、前記認証装置よりチャレンジデータを受け取るチャレンジデータ受取手段と、前記証明情報を用いて前記チャレンジデータからレスポンスデータを生成するレスポンスデータ生成手段と、生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力手段とを備えることを特徴とする。

【００３１】

この構成によると、認証記録媒体は、証明情報を用いて、認証装置より受け取ったチャレンジデータからレスポンスデータを生成し、生成したレスポンスデータを認証装置へ出力することができる。このとき、レスポンスデータを生成する際に用いる証明情報は、耐タンパ性を有する証明情報記憶手段にて記憶されているため、第三者にて改竄されることはない。これにより、認証記録媒体は、証明情報を用いて生成したレスポンスデータを自己の正当性を証明するデータとすることができる。また、自己の正当性を証明するために認証情報そのものを認証装置へ出力する代わりに、レスポンスデータを認証装置へ出力しているため、認証記録媒体と認証装置との間におけるデータ盗聴に対するセキュリティが向上される。

【００３２】

ここで、前記認証記録媒体は、宅配業者が有し、前記認証記録媒体は、さらに、宅配業者による訪問を示す訪問情報を記憶している訪問情報記憶手段と、前記訪問情報を前記認証装置へ出力する訪問情報出力手段とを備えるとしてもよい。

この構成によると、認証記録媒体は、さらに、訪問情報を認証装置へ出力することができる。

【００３３】

ここで、前記証明情報は、暗号化鍵であり、前記レスポンスデータ生成手段は、前記暗号化鍵を用いて前記チャレンジデータを暗号して、レスポンスデータを生成するとしてもよい。

この構成によると、認証記録媒体は、暗号鍵を用いて、チャレンジデータを暗号化したレスポンスデータを生成することができる。

【００３４】

ここで、前記暗号化鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報であり、前記レスポンスデータ生成手段は、前記所有者証明情報を用いて、前記チャレンジデータを暗号化して、レスポンスデータを生成するとしてもよい。

この構成によると、暗号鍵を認証記録媒体の所有者の生体科学的特徴を示す情報として、レスポンスデータを生成することができる。

【００３５】

ここで、前記認証情報は、秘密鍵であり、前記チャレンジデータは、前記秘密鍵に対応する公開鍵を用いて、前記認証装置により生成されたデータが暗号化されたデータであり、前記レスポンスデータ生成手段は、前記秘密鍵を用いて受け取ったチャレンジデータを復号して、レスポンスデータを生成するとしてもよい。

この構成によると、認証記録媒体は、秘密鍵を用いて、認証装置より受け取ったチャレンジデータを復号して、レスポンスデータを生成することができる。つまり、公開鍵暗号を利用して、レスポンスデータを生成することができる。

【００３６】

ここで、前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応した鍵であり、前記公開鍵は、前記所有者証明情報に対応する前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を用いて前記認証記録媒体にて生成された鍵であるとしてもよい。

この構成によると、認証記録媒体は、当該認証記録媒体の所有者の生体科学的特徴を示す情報に対応する秘密鍵を用いて、レスポンスデータを生成することができる。

【００３７】
ここで、前記認証情報は、秘密鍵であり、前記レスポンスデータ生成手段は、前記秘密鍵を用いて受け取ったチャレンジデータの電子署名であるレスポンスデータを生成するとしてもよい。
この構成によると、認証記録媒体は、レスポンスデータとして、チャレンジデータの電子署名を生成することができる。
【００３８】
ここで、前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応した鍵であるとしてもよい。
この構成によると、認証記録媒体は、当該認証記録媒体の所有者の生体科学的特徴を示す情報に対応する秘密鍵を用いて、チャレンジデータの電子署名を生成することができる。
【００３９】
ここで、前記チャレンジデータ受取手段は、前記チャレンジデータを受け取る代わりに、前記チャレンジデータから生成された変換チャレンジ情報を受け取り、受け取った変換チャレンジ情報より前記チャレンジデータを生成するとしてもよい。
この構成によると、認証記録媒体は、チャレンジデータの代わりに、チャレンジデータより生成された変換チャレンジ情報を認証装置より受け取り、受け取った変換チャレンジ情報よりチャレンジデータを生成することができる。
【００４０】
ここで、前記変換チャレンジ情報は、光信号、バーコード、ＱＲコード、赤外線信号、及び音声信号のうち何れかからなる情報であるとしてもよい。
この構成によると、認証記録媒体は、光信号、バーコード、ＱＲコード、赤外線信号、及び音声信号のうち何れかからなる変換チャレンジ情報を、認証装置より受け取り、受け取った変換チャレンジ情報よりチャレンジデータを生成することができる。
【００４１】
ここで、前記レスポンスデータ出力手段は、前記レスポンスデータを出力する代わりに、前記レスポンスデータから変換レスポンス情報を生成し、生成した変換レスポンス情報を出力するとしてもよい。
この構成によると、認証記録媒体は、レスポンスデータの代わりに、レスポンスデータより生成した変換レスポンス情報を認証装置へ出力することができる。
【００４２】
ここで、前記変換レスポンス情報は、光信号、バーコード、ＱＲコード、赤外線信号、及び音声信号のうち何れかからなる情報であるとしてもよい。
この構成によると、認証記録媒体は、光信号、バーコード、ＱＲコード、赤外線信号、及び音声信号のうち何れかからなる変換レスポンス情報を、認証装置へ出力することができる。
【００４３】
ここで、前記認証記録媒体は、さらに、前記認証装置より、前記認証装置を識別する装置識別子を受け取る識別子受取手段と、受け取った装置識別子を記憶する識別子記憶手段とを備えるとしてもよい。
この構成によると、認証記録媒体は、認証装置より装置識別子を受け取り、記憶することができる。
【発明を実施するための最良の形態】
【００４４】
１．第１の実施の形態
本発明に係る第１の実施の形態としての身元認証システム１について説明する。
１．１　身元認証システム１の概要
身元認証システム１は、図１に示すように、認証カード１０、１１、・・・、１２とユーザ端末２０とカードリーダ３０とから構成されている。

【００４５】
認証カード１０、１１、・・・、１２は、それぞれ利用者宅へ訪問する異なる訪問業者（例えば、宅配便の業者）が所有するカードである。認証カード１０には、認証カード１０自身の正当性を証明するための訪問業者固有の身元証明鍵を予め記憶している。つまり、認証カード１１、・・・、１２には、認証カード１０に記憶されている身元証明鍵とは異なる身元証明鍵がそれぞれ予め記憶されていることになる。身元証明鍵は、訪問業者にて安全に管理されている。なお、ここでは、身元認証システム１の概要についての説明を認証カード１０とユーザ端末２０とカードリーダ３０とを用いて行う。
【００４６】
ユーザ端末２０及びカードリーダ３０は、訪問業者から配布された装置であり、ユーザ端末２０には、認証カード１０の正当性を検証するための身元認証鍵が予め記憶されている。
ユーザ端末２０は、利用者の宅内に配置されており、カードリーダ３０は、利用者の宅外（例えば、玄関先）に配置されており、ユーザ端末２０とカードリーダ３０とは、ケーブル４０にて接続されている。
【００４７】
身元認証システム１は、認証カード１０がカードリーダ３０に挿入されると、認証カード１０に記憶している身元証明鍵と、ユーザ端末２０に記憶している身元認証鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行い、認証結果をユーザ端末２０の表示部２０３にて表示する。
なお、ここで用いる暗号処理は、秘密鍵による暗号処理である。秘密鍵による暗号処理の一例は、ＤＥＳである。ＤＥＳについては、公知であるので説明を省略するが、身元証明鍵と身元認証鍵とが同一の鍵となることは、言うまでもない。
【００４８】
また、身元認証システム１において、認証カード１１、・・・、１２のうち何れかの認証カードがカードリーダ３０に挿入された場合も同様の動作を行うため、説明は省略する。
１．２　認証カード１０の構成
ここでは、認証カード１０の構成について説明する。認証カード１０は、ＩＣを内蔵している可搬型の記録媒体であり、一例として、ＩＣカード機能付メモリカードである。認証カード１０は、図２に示すように、証明鍵記憶部１０１、制御部１０２及び入出力部１０３から構成されている。
【００４９】
認証カード１０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＲＯＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード１０は、その機能を達成する。
なお、認証カード１１、・・・、１２は、認証カード１０と同様の構成を有しているため、説明は省略する。
【００５０】
（１）　証明鍵記憶部１０１
証明鍵記憶部１０１は、耐タンパ性を有しており、身元証明鍵と、身元証明鍵を識別する証明鍵ＩＤとからなる組を１つ記憶している。上述したように、ここで記憶されている身元証明鍵は、認証カード１０自身の正当性を証明するための訪問業者固有の鍵であり、訪問業者にて安全に管理されている。
【００５１】
以降の説明において、必要に応じて、身元証明鍵として「ＳＫ１」を用いて説明する。
（２）　制御部１０２
制御部１０２は、カードリーダ３０より入出力部１０３を介して、証明鍵ＩＤを要求する旨のＩＤ要求情報を受け取ると、証明鍵記憶部１０１より証明鍵ＩＤを取得し、取得し

た証明鍵ＩＤを入出力部１０３を介してカードリーダ３０へ出力する。

【００５２】

さらに、制御部１０２は、カードリーダ３０より乱数「Ｎ」を受け取ると、証明鍵記憶部１０１より身元証明鍵「ＳＫ１」を取得し、取得した身元証明鍵「ＳＫ１」を用いて、カードリーダ３０より受け取った乱数「Ｎ」に対して暗号化を施し、暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を生成する。制御部１０２は、生成した暗号化情報を入出力部１０３を介してカードリーダ３０へ出力する。ここで、Ｅｎｃ（ＳＫ１、Ｎ）は、乱数「Ｎ」が身元証明鍵「ＳＫ１」にて暗号化された情報であることを意味する。

【００５３】

（３）　入出力部１０３

入出力部１０３は、カードリーダ３０より受け取った情報を制御部１０２へ出力し、制御部１０２から受け取った情報をカードリーダ３０へ出力する。

１．３　ユーザ端末２０の構成

ここでは、ユーザ端末２０の構成について説明する。ユーザ端末２０は、カードリーダ３０に挿入された認証カード１０の認証を行う。ユーザ端末２０は、図３に示すように、認証鍵記憶部２０１、認証部２０２、表示部２０３及び入出力部２０４から構成されている。

【００５４】

ユーザ端末２０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記ＲＯＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末２０は、その機能を達成する。

【００５５】

（１）　認証鍵記憶部２０１

認証鍵記憶部２０１は、耐タンパ性を有しており、図４に一例として示すように、鍵情報テーブルＴ１００を備えている。

鍵情報テーブルＴ１００は、身元認証鍵と認証鍵ＩＤとからなる組を複数記憶するための領域を備えている。

【００５６】

身元認証鍵は、カードリーダ３０の挿入された認証カードの正当性を検証するための鍵であり、上述したように身元証明鍵と同一のものである。

認証鍵ＩＤは、身元認証鍵を識別する識別子であり、証明鍵ＩＤと同一の識別子にて対応付けされている。これにより、身元認証鍵と身元証明鍵との対応付けが可能となる。

また、鍵情報テーブルＴ１００にて記憶されている身元認証鍵の個数は、訪問業者の数と同じ数である。

【００５７】

つまり、認証カード１０、１１、・・・、１２のそれぞれに記憶されている証明鍵ＩＤと身元証明鍵との組に対応する、認証鍵ＩＤと身元認証鍵とからなる組が記憶されている。

（２）　認証部２０２

認証部２０２は、乱数を記憶する乱数記憶領域２５０及びカードリーダ３０より入出力部２０４を介して受け取った証明鍵ＩＤを記憶するＩＤ記憶領域２５１を有している。

【００５８】

認証部２０２は、カードリーダ３０より入出力部２０４を介して、カードリーダ３０に認証カード１０が挿入されたことを検知した旨を示す検知情報と、証明鍵ＩＤとを受け取り、受け取った証明鍵ＩＤをＩＤ記憶領域２５１に記憶する。次に、認証部２０２は、乱数「Ｎ」を生成し、生成した乱数「Ｎ」を入出力部２０４を介してカードリーダ３０へ出力し、生成した乱数「Ｎ」を乱数記憶領域２５０に記憶する。

【００５９】

さらに、認証部２０２は、カードリーダ３０より入出力部２０４を介して、暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を受け取る。次に、ＩＤ記憶領域２５１にて記憶している証明鍵ＩＤと一致する認証鍵ＩＤと対応する身元認証鍵を鍵情報テーブルＴ１００より取得し、取得した身元認証鍵を用いて、暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）の復号を行い、復号により得られた復号結果と、乱数記憶領域２５０にて記憶している乱数「Ｎ」とが一致するか否かを判断する。

【００６０】

復号結果と乱数「Ｎ」とが一致する場合には、認証部２０２は、カードリーダ３０に挿入された認証カードが正当な認証カードであると認証し、認証結果として訪問者が正当な訪問者である旨を示す正当訪問者情報を生成し、生成した正当訪問者情報を表示部２０３へ出力する。復号結果と乱数「Ｎ」とが一致しない場合には、認証部２０２は、カードリーダ３０に挿入された認証カードが不正な認証カードであると認証し、認証結果として訪問者が不正な訪問者である旨を示す不正訪問者情報を生成し、生成した不正訪問者情報を表示部２０３へ出力する。さらに、認証部２０２は、乱数記憶領域２５０に記憶している乱数「Ｎ」の消去、及びＩＤ記憶領域２５１に記憶している証明鍵ＩＤの消去を行う。

【００６１】

（３）　表示部２０３

表示部２０３は、例えば、ディスプレイを備え、認証部２０２より受け取った認証結果の情報を外部に対して表示する。

（４）　入出力部２０４

入出力部２０４は、カードリーダ３０より受け取った情報を認証部２０２へ出力し、認証部２０２から受け取った情報をカードリーダ３０へ出力する。

【００６２】

１．４　カードリーダ３０

カードリーダ３０は、図３に示すように、カード読取部３０１及び入出力部３０２から構成されている。

カードリーダ３０は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＲＯＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、カードリーダ３０は、その機能を達成する。

【００６３】

（１）　カード読取部３０１

カード読取部３０１は、認証カード１０が挿入されたことの検知を行う。カード読取部３０１は、認証カード１０が挿入されたことを検知すると、検知情報及びＩＤ要求情報を生成し、生成したＩＤ要求情報を認証カード１０へ出力する。次に、認証カード１０より証明鍵ＩＤを受け取ると、受け取った証明鍵ＩＤと、生成した検知情報とを入出力部３０２を介してユーザ端末２０へ出力する。

【００６４】

さらに、カード読取部３０１は、ユーザ端末２０より入出力部３０２を介して、乱数「Ｎ」を受け取ると、受け取った乱数「Ｎ」を認証カード１０へ出力する。カード読取部３０１は、認証カード１０より暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を受け取ると、受け取った暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を入出力部３０２を介してユーザ端末２０へ出力する。

（２）　入出力部３０２

入出力部３０２は、ユーザ端末２０より受け取った情報をカード読取部３０１へ出力し、カード読取部３０１から受け取った情報をユーザ端末２０へ出力する。

【００６５】

１．５　身元認証処理の動作

ここでは、認証カード１０がカードリーダ３０に挿入されてからユーザ端末２０にて認証を行うまでの処理である身元認証処理の動作について、図５に示す流れ図を用いて説明する。

カードリーダ３０は、認証カード１０が挿入されたことを検知すると（ステップＳ５）、検知情報及びＩＤ要求情報を生成し、生成したＩＤ要求情報を認証カード１０へ出力する（ステップＳ１０）。

【００６６】

認証カード１０は、カードリーダ３０よりＩＤ要求情報を受け取ると、証明鍵記憶部１０１にて記憶している証明鍵ＩＤを取得し、取得した証明鍵ＩＤをカードリーダ３０へ出力する（ステップＳ１５）。

カードリーダ３０は、認証カード１０より証明鍵ＩＤを受け取ると（ステップＳ２０）、受け取った証明鍵ＩＤと、ステップＳ１０にて生成した検知情報とをユーザ端末２０へ出力する（ステップＳ２５）。

【００６７】

ユーザ端末２０は、カードリーダ３０より証明鍵ＩＤと検知情報とを受け取ると、受け取った証明鍵ＩＤをＩＤ記憶領域２５１に記憶する（ステップＳ３０）。次に、ユーザ端末２０は、乱数「Ｎ」を生成し、生成した乱数「Ｎ」をカードリーダ３０へ出力し、さらに、生成した乱数「Ｎ」を乱数記憶領域２５０に記憶する（ステップＳ３５）。

カードリーダ３０は、ユーザ端末２０より乱数「Ｎ」を受け取ると、受け取った乱数「Ｎ」を認証カード１０へ出力する（ステップＳ４０）。

【００６８】

認証カード１０は、カードリーダ３０より乱数「Ｎ」を受け取ると（ステップＳ４５）、受け取った乱数「Ｎ」を証明鍵記憶部１０１にて記憶している身元証明鍵を用いて暗号化し、暗号化情報を生成し、生成した暗号化情報をカードリーダ３０へ出力する（ステップＳ５０）。

カードリーダ３０は、認証カード１０より暗号化情報を受け取ると、受け取った暗号化情報をユーザ端末２０へ出力する（ステップＳ５５）。

【００６９】

ユーザ端末２０は、カードリーダ３０より暗号化情報を受け取ると、受け取った暗号化情報と認証鍵記憶部２０１にて記憶している身元認証鍵とを用いて、認証処理を行う（ステップＳ６０）。

１．６　認証処理

ここでは、身元認証処理のステップＳ６０にて行われる認証処理について、図６に示す流れ図を用いて説明する。

【００７０】

ユーザ端末２０は、認証カード１０よりカードリーダ３０を介して暗号化情報を受け取る（ステップＳ１００）。次に、ユーザ端末２０は、身元認証処理のステップＳ３０にてＩＤ記憶領域２５１に記憶した証明鍵ＩＤと一致する認証鍵ＩＤと対応付けられた身元認証鍵を鍵情報テーブルＴ１００より取得する（ステップＳ１０５）。さらに、ユーザ端末２０は、取得した身元認証鍵を用いて、ステップＳ１００にて受け取った暗号化情報を復号する（ステップＳ１１０）。

【００７１】

次に、ユーザ端末２０は、復号して得られた復号結果と、身元認証処理のステップＳ３５にて乱数記憶領域２５０に記憶した乱数「Ｎ」とが一致するか否かの判断を行う（ステップＳ１１５）。

一致すると判断する場合には（ステップＳ１１５における「ＹＥＳ」）、正当訪問者情報を生成し、生成した正当訪問者情報を表示し（ステップＳ１２０）、乱数記憶領域２５０に記憶している乱数「Ｎ」、及びＩＤ記憶領域２５１に記憶している証明鍵ＩＤをそれぞれ消去し（ステップＳ１３０）、処理を終了する。

【００７２】

一致しないと判断する場合には（ステップＳ１１５における「ＮＯ」）、不正訪問者情報を生成し、生成した不正訪問者情報を表示し（ステップＳ１２５）、乱数記憶領域２５０に記憶している乱数「Ｎ」、及びＩＤ記憶領域２５１に記憶している証明鍵ＩＤをそれ

ぞれ消去し（ステップＳ１３０）、処理を終了する。

２．第２の実施の形態

ここでは、本発明に係る第２の実施の形態としての身元認証システム１Ａについて説明する。

【００７３】

身元認証システム１では、身元認証鍵をユーザ端末２０の認証鍵記憶部２０１に予め記憶したが、身元認証システム１Ａでは、ユーザ端末が利用者に配布された後に、訪問業者より身元認証鍵を配布する。

２．１　身元認証システム１Ａの概要

身元認証システム１Ａは、図７に示すように、認証カード１０Ａ、１１Ａ、・・・、１２Ａと、ユーザ端末２０Ａと、カードリーダ３０Ａと、配信装置５０Ａとから構成されている。カードリーダ３０Ａとユーザ端末２０Ａとは、ケーブル４０Ａにて接続されている。

【００７４】

認証カード１０Ａ、１１Ａ、・・・、１２Ａは、訪問業者より利用者宅へ訪問する訪問者一人一人に割り当てられており、各認証カードには、それぞれ異なる身元証明鍵を予め記憶している。つまり、利用者宅へ訪問する訪問者と身元証明鍵とが対応付けられていることになる。

ここで、図７には、図示していないが、ユーザ端末２０Ａと同様の構成を有するユーザ端末２１Ａ、・・・、２２Ａも配信装置５０Ａとインターネットを介して接続されている。また、ユーザ端末２１Ａ、・・・、２２Ａはカードリーダ３０Ａと同様の構成を有するカードリーダ３１Ａ、・・・、３２Ａとそれぞれ接続されている。

【００７５】

ここでは、認証カード１０Ａとユーザ端末２０Ａとカードリーダ３０Ａとを用いて、身元認証システム１Ａの概要について説明する。なお、認証カード１１Ａ、・・・、１２Ａは、認証カード１０Ａと同様であり、ユーザ端末２１Ａ、・・・、２２Ａは、ユーザ端末２０Ａと同様であり、カードリーダ３１Ａ、・・・、３２Ａは、カードリーダ３０Ａと同様であるため、説明は省略する。

【００７６】

身元認証システム１Ａでは、訪問業者が利用者宅へ訪問する前に、訪問者に対応する身元認証鍵をユーザ端末２０Ａへインターネットを介して送信する。認証カード１０Ａがカードリーダ３０Ａに挿入されると、ユーザ端末２０Ａは、認証カード１０Ａに記憶されている身元証明鍵と、配信装置５０Ａより事前に受信して記憶している身元認証鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行い、認証結果を表示部２０３Ａにて表示する。

【００７７】

ここで用いる暗号処理は、身元認証システム１と同様に秘密鍵による暗号処理である。また、身元認証システム１と同様に身元証明鍵と身元認証鍵とが同一の鍵となることは、言うまでもない。

２．２　配信装置５０Ａ

配信装置５０Ａは、訪問者が利用者宅へ訪問する前に、訪問者に対応する身元認証鍵をユーザ端末２０Ａへ送信する装置である。配信装置５０Ａは、図８に示すように、配信鍵記憶部５０１Ａ、制御部５０２Ａ、操作部５０３Ａ及び送信部５０４Ａから構成されている。

【００７８】

配信装置５０Ａは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、モデムなどからなどから構成されるコンピュータシステムである。前記ＲＯＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、配信装置５０Ａは、その機能を達成する。

【００７９】
（１）　配信鍵記憶部５０１Ａ
配信鍵記憶部５０１Ａは、図９に一例として示すように、配信鍵情報テーブルＴ２００を備えている。
配信鍵情報テーブルＴ2.００は、訪問者ＩＤと身元認証鍵とからなる組を複数記憶するための領域を備えている。
【００８０】
訪問者ＩＤは、訪問者を識別する識別子であり、身元認証鍵は、身元証明鍵と同一の鍵であり、訪問者ＩＤと対応付けられている。
なお、ここで記憶されている身元認証鍵の個数は、訪問者の人数、つまり認証カードの個数と同一となる。
また、身元認証鍵と訪問者ＩＤとを対応付けることにより、訪問者ＩＤに対応する身元認証鍵を記憶している認証カードを訪問者に割り当てることができる。
【００８１】
（２）　制御部５０２Ａ
制御部５０２Ａは、操作部５０３Ａより、身元認証鍵の登録を示す情報と、訪問者ＩＤと、身元認証鍵とを受け取ると、受け取った訪問者ＩＤと身元認証鍵とを対応付けて、配信鍵記憶部５０１Ａへ書き込む。
制御部５０２Ａは、操作部５０３Ａより身元認証鍵をユーザ端末２０Ａへ配信する旨の情報と、訪問者ＩＤとからなる配信情報を受け取ると、受け取った配信情報に含まれる訪問者ＩＤと対応する身元認証鍵を配信鍵情報テーブルＴ２００より取得する。制御部５０２Ａは、取得した身元認証鍵をユーザ端末２０Ａへ送信部５０４Ａを介して送信する。
【００８２】
（３）　操作部５０３Ａ
操作部５０３Ａは、配信装置５０Ａの操作者の操作により、身元認証鍵の登録を示す情報と、訪問者ＩＤと、身元認証鍵とを受け付けると、受け付けた身元認証鍵の登録を示す情報と、訪問者ＩＤと、身元認証鍵とを制御部５０２Ａへ出力する。
また、操作部５０３Ａは、操作者の操作により、配信情報を受け付けると、受け付けた配信情報を制御部５０２Ａへ出力する。
【００８３】
なお、操作者は、利用者宅へ訪問する訪問者自身に限らず、訪問業者に属する者であればよい。
（４）　送信部５０４Ａ
送信部５０４Ａは、制御部５０２Ａより受け取った情報をユーザ端末２０Ａへインターネットを介して出力する。
【００８４】
２．３　認証カード１０Ａ
ここでは、認証カード１０Ａの構成について説明する。認証カード１０Ａは、ＩＣを内蔵している可搬型の記録媒体であり、一例として、ＩＣカード機能付メモリカードである。認証カード１０Ａは、図１０に示すように、証明鍵記憶部１０１Ａ、制御部１０２Ａ及び入出力部１０３Ａから構成されている。
【００８５】
認証カード１０Ａは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＲＯＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード１０Ａは、その機能を達成する。
なお、認証カード１１Ａ、・・・、１２Ａは、認証カード１０Ａと同様の構成を有しているため、説明は省略する。
【００８６】
（１）　証明鍵記憶部１０１Ａ

証明鍵記憶部１０１Ａは、耐タンパ性を有しており、訪問者に対応する身元証明鍵を１つ記憶している。

以降の説明において、必要に応じて、身元証明鍵として「ＳＫ１」を用いて説明する。

（２）　制御部１０２Ａ

制御部１０２Ａは、カードリーダ３０Ａより乱数「Ｎ」を受け取ると、証明鍵記憶部１０１Ａより身元証明鍵「ＳＫ１」を取得し、取得した身元証明鍵「ＳＫ１」を用いて、カードリーダ３０Ａより受け取った乱数「Ｎ」に対して暗号化を施し、暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を生成する。制御部１０２Ａは、生成した暗号化情報を入出力部１０３Ａを介してカードリーダ３０Ａへ出力する。

【００８７】

（３）　入出力部１０３Ａ

入出力部１０３Ａは、認証カード１０の入出力部１０３と同様であるため、説明は省略する。

２．４　ユーザ端末２０Ａの構成

ここでは、ユーザ端末２０Ａの構成について説明する。ユーザ端末２０Ａは、図１１に示すように、認証鍵記憶部２０１Ａ、認証部２０２Ａ、表示部２０３Ａ、入出力部２０４Ａ及び受信部２０５Ａから構成されている。

【００８８】

ユーザ端末２０Ａは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記ＲＯＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末２０Ａは、その機能を達成する。

【００８９】

また、上記の身元認証システム１Ａの概要にて示したように、ユーザ端末２１Ａ、・・・、２２Ａは、ユーザ端末２０Ａと同様の構成であるため、説明は省略する。

（１）　認証鍵記憶部２０１Ａ

認証鍵記憶部２０１Ａは、耐タンパ性を有しており、配信装置５０Ａよりインターネットを介して受信した身元認証鍵を記憶する領域を有している。

【００９０】

（２）　受信部２０５Ａ

受信部２０５Ａは、配信装置５０Ａよりインターネットを介して、身元認証鍵を受信すると、受信した身元認証鍵を認証鍵記憶部２０１Ａへ書き込む。

これにより、ユーザ端末２０Ａは、訪問者に対応する身元認証鍵を事前に記憶することができる。

【００９１】

（３）　認証部２０２Ａ

認証部２０２Ａは、乱数を記憶する乱数記憶領域２５０Ａを有している。

認証部２０２Ａは、カードリーダ３０Ａより入出力部２０４Ａを介して、カードリーダ３０Ａに認証カード１０Ａが挿入されたことを検知した旨を示す検知情報を受け取ると、乱数「Ｎ」を生成し、生成した乱数「Ｎ」を入出力部２０４Ａを介してカードリーダ３０Ａへ出力し、生成した乱数「Ｎ」を乱数記憶領域２５０Ａに記憶する。

【００９２】

さらに、認証部２０２Ａは、カードリーダ３０Ａより入出力部２０４Ａを介して、暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を受け取ると、認証鍵記憶部２０１Ａにて事前に記憶している身元認証鍵を認証鍵記憶部２０１Ａより取得し、取得した身元認証鍵を用いて、暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）の復号を行い、復号により得られた復号結果と、乱数記憶領域２５０Ａにて記憶している乱数「Ｎ」とが一致するか否かを判断する。

【００９３】

復号結果と乱数「Ｎ」とが一致する場合には、認証部２０２Ａは、カードリーダ３０Ａ

に挿入された認証カードが正当な認証カードであると認証し、認証結果として訪問者が正当な訪問者である旨を示す正当訪問者情報を生成し、生成した正当訪問者情報を表示部２０３Ａへ出力する。復号結果と乱数「Ｎ」とが一致しない場合には、認証部２０２Ａは、カードリーダ３０Ａに挿入された認証カードが不正な認証カードであると認証し、認証結果として訪問者が不正な訪問者である旨を示す不正訪問者情報を生成し、生成した不正訪問者情報を表示部２０３Ａへ出力する。さらに、認証部２０２Ａは、認証鍵記憶部２０１Ａにて記憶している身元認証鍵の消去及び乱数記憶領域２５０Ａに記憶している乱数「Ｎ」の消去を行う。

【００９４】

（４）　表示部２０３Ａ

表示部２０３Ａは、ユーザ端末２０の表示部２０３と同様であるため、説明は省略する。

（５）　入出力部２０４Ａ

入出力部２０４Ａは、ユーザ端末２０の入出力部２０４と同様であるため、説明は省略する。

【００９５】

２．５　カードリーダ３０Ａ

カードリーダ３０Ａは、図１１に示すように、カード読取部３０１Ａ及び入出力部３０２Ａから構成されている。

カードリーダ３０Ａは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＲＯＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、カードリーダ３０Ａは、その機能を達成する。

【００９６】

なお、上記の身元認証システム１Ａの概要にて示したように、カードリーダ３１Ａ、・・・、３２Ａは、カードリーダ３０Ａと同様の構成であるため、説明は省略する。

（１）　カード読取部３０１Ａ

カード読取部３０１Ａは、認証カード１０Ａが挿入されたことの検知を行う。カード読取部３０１Ａは、認証カード１０Ａが挿入されたことを検知すると、検知情報を生成し、生成した検知情報を入出力部３０２Ａを介してユーザ端末２０Ａへ出力する。

【００９７】

さらに、カード読取部３０１Ａは、ユーザ端末２０Ａより入出力部３０２Ａを介して、乱数「Ｎ」を受け取ると、受け取った乱数「Ｎ」を認証カード１０Ａへ出力する。カード読取部３０１Ａは、認証カード１０Ａより暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を受け取ると、受け取った暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を入出力部３０２Ａを介してユーザ端末２０Ａへ出力する。

【００９８】

（２）　入出力部３０２Ａ

入出力部３０２Ａは、カードリーダ３０の入出力部３０２と同様であるため、説明は省略する。

２．６　配信処理の動作

ここでは、身元認証鍵を事前に配信する配信処理について、図１２に示す流れ図を用いて、説明する。

【００９９】

配信装置５０Ａは、利用者の操作により配信情報を受け付けると（ステップＳ２００）、受け付けた配信情報に含まれる訪問者ＩＤに対応する身元認証鍵を配信鍵記憶部５０１Ａより取得する（ステップＳ２０５）。次に、配信装置５０Ａは、取得した身元認証鍵をユーザ端末２０Ａへインターネットを介して配信する（ステップＳ２１０）。

ユーザ端末２０Ａは、配信装置５０Ａより身元認証鍵を受信すると（ステップＳ２１５）、受信した身元認証鍵を認証鍵記憶部２０１Ａへ書き込む（ステップＳ２２０）。

【０１００】
２．７　身元認証処理の動作
ここでは、認証カード１０Ａがカードリーダ３０Ａに挿入されてからユーザ端末２０Ａにて認証を行うまでの処理である身元認証処理の動作について、図１３に示す流れ図を用いて説明する。
カードリーダ３０Ａは、認証カード１０Ａが挿入されたことを検知すると（ステップＳ２５０）、検知情報を生成し、生成した検知情報をユーザ端末２０Ａへ出力する（ステップＳ２５５）。
【０１０１】
ユーザ端末２０Ａは、カードリーダ３０Ａより検知情報を受け取ると、乱数「Ｎ」を生成し、生成した乱数「Ｎ」をカードリーダ３０Ａへ出力し、さらに、生成した乱数「Ｎ」を乱数記憶領域２５０Ａに記憶する（ステップＳ２６０）。
カードリーダ３０Ａは、ユーザ端末２０Ａより乱数「Ｎ」を受け取ると、受け取った乱数「Ｎ」を認証カード１０Ａへ出力する（ステップＳ２６５）。
【０１０２】
認証カード１０Ａは、カードリーダ３０Ａより乱数「Ｎ」を受け取ると（ステップＳ２７０）、受け取った乱数「Ｎ」を証明鍵記憶部１０１Ａにて記憶している身元証明鍵を用いて暗号化して、暗号化情報を生成し、生成した暗号化情報をカードリーダ３０Ａへ出力する（ステップＳ２７５）。
カードリーダ３０Ａは、認証カード１０Ａより暗号化情報を受け取ると、受け取った暗号化情報をユーザ端末２０Ａへ出力する（ステップＳ２８０）。
【０１０３】
ユーザ端末２０Ａは、カードリーダ３０Ａより暗号化情報を受け取ると、受け取った暗号化情報と認証鍵記憶部２０１Ａにて記憶している身元認証鍵とを用いて、認証処理を行う（ステップＳ２８５）。
２．８　認証処理
ここでは、身元認証処理のステップＳ２８５にて行われる認証処理について、図１４に示す流れ図を用いて説明する。
【０１０４】
ユーザ端末２０Ａは、認証カード１０Ａよりカードリーダ３０Ａを介して暗号化情報を受け取る（ステップＳ３００）。次に、ユーザ端末２０Ａは、配信装置５０Ａより事前に配信された身元認証鍵を認証鍵記憶部２０１Ａより取得する（ステップＳ３０５）。さらに、ユーザ端末２０Ａは、取得した身元認証鍵を用いて、ステップＳ３００にて受け取った暗号化情報を復号する（ステップＳ３１０）。
【０１０５】
次に、ユーザ端末２０Ａは、復号して得られた復号結果と、身元認証処理のステップＳ２６０にて乱数記憶領域２５０Ａに記憶した乱数「Ｎ」とが一致するか否かの判断を行う（ステップＳ３１５）。
一致すると判断する場合には（ステップＳ３１５における「ＹＥＳ」）、正当訪問者情報を生成し、生成した正当訪問者情報を表示し（ステップＳ３２０）、認証鍵記憶部２０１Ａにて記憶している身元認証鍵及び乱数記憶領域２５０Ａに記憶している乱数「Ｎ」を消去し（ステップＳ３３０）、処理を終了する。
【０１０６】
一致しないと判断する場合には（ステップＳ３１５における「ＮＯ」）、不正訪問者情報を生成し、生成した不正訪問者情報を表示し（ステップＳ３２５）、認証鍵記憶部２０１Ａにて記憶している身元認証鍵及び乱数記憶領域２５０Ａに記憶している乱数「Ｎ」を消去し（ステップＳ３３０）、処理を終了する。
３．第３の実施の形態
ここでは、本発明に係る第３の実施の形態としての身元認証システム１Ｂについて説明する。

【０１０７】
身元認証システム１Ｂでは、訪問者が利用者宅に訪問時に、身元認証鍵として訪問者の生体科学的特徴を示すバイオメトリックス情報を用いて、認証カードが正当な認証カードであるか否かの認証を行う。

３．１　身元認証システム１Ｂの概要

身元認証システム１Ｂは、図１５に示すように、認証カード１０Ｂ、１１Ｂ、・・・、１２Ｂとユーザ端末２０Ｂとカードリーダ３０Ｂとから構成されている。カードリーダ３０Ｂとユーザ端末２０Ｂとは、ケーブル４０Ｂにて接続されている。

【０１０８】
認証カード１０Ｂ、１１Ｂ、・・・、１２Ｂは、訪問業者より利用者宅へ訪問する訪問者一人一人に割り当てられており、割り当てられた訪問者のバイオメトリックス情報を身元証明鍵として予め記憶している。ここで、バイオメトリックス情報は訪問者の指紋模様の特徴点からなる身元証明指紋情報とする。つまり、認証カード１０Ｂ、１１Ｂ、・・・、１２Ｂには、それぞれ異なる身元証明鍵が記憶されていることになる。

【０１０９】
カードリーダ３０Ｂは、訪問者より指紋の入力を受け付ける指紋読取部３１０Ｂを有している。

ここでは、認証カード１０Ｂとユーザ端末２０Ｂとカードリーダ３０Ｂとを用いて、身元認証システム１Ｂの概要について説明する。なお、認証カード１１Ｂ、・・・、１２Ｂは、認証カード１０Ｂと同様であるため、説明は省略する。

【０１１０】
身元認証システム１Ｂは、認証カード１０Ｂがカードリーダ３０Ｂに挿入されると、訪問者に対して指紋の入力を要求する。身元認証システム１Ｂは、カードリーダ３０Ｂの指紋読取部３１０Ｂより指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報と認証カード１０Ｂに記憶している身元証明鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行い、認証結果をユーザ端末２０Ｂの表示部２０３Ｂにて表示する。

【０１１１】
ここで用いる暗号処理は、身元認証システム１と同様に秘密鍵による暗号処理である。また、身元認証システム１と同様に身元証明鍵と身元認証指紋情報とが同一の鍵となることは、言うまでもない。

また、身元認証システム１Ｂにおいて、認証カード１１Ｂ、・・・、１２Ｂのうち何れかの認証カードがカードリーダ３０Ｂに挿入された場合も同様の動作を行うため、説明は省略する。

【０１１２】
３．２　認証カード１０Ｂ

ここでは、認証カード１０Ｂの構成について説明する。認証カード１０Ｂは、ＩＣを内蔵している可搬型の記録媒体であり、一例として、ＩＣカード機能付メモリカードである。認証カード１０Ｂは、図１６に示すように、証明鍵記憶部１０１Ｂ、制御部１０２Ｂ及び入出力部１０３Ｂから構成されている。

【０１１３】
認証カード１０Ｂは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＲＯＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード１０Ｂは、その機能を達成する。

なお、認証カード１１Ｂ、・・・、１２Ｂは、認証カード１０Ｂと同様の構成を有しているため、説明は省略する。

【０１１４】
（１）　証明鍵記憶部１０１Ｂ

証明鍵記憶部１０１Ｂは、耐タンパ性を有しており、訪問者に対応する身元証明指紋情

報を身元証明鍵として１つ記憶している。
以降の説明において、必要に応じて、身元証明鍵として「ＳＫ１」を用いて説明する。
（２）　制御部１０２Ｂ
制御部１０２Ｂは、第２の実施の形態にて示した認証カード１０Ａの制御部１０２Ａと同様であるため、説明は省略する。
【０１１５】
（３）　入出力部１０３Ｂ
入出力部１０３Ｂは、第２の実施の形態にて示した認証カード１０Ａの入出力部１０３Ａと同様であるため、説明は省略する。つまり、入出力部１０３Ｂは、第１の実施の形態にて示した認証カード１０の入出力部１０３とも同様である。
３．３　ユーザ端末２０Ｂの構成
ここでは、ユーザ端末２０Ｂの構成について説明する。ユーザ端末２０Ｂは、図１７に示すように、認証鍵記憶部２０１Ｂ、認証部２０２Ｂ、表示部２０３Ｂ及び入出力部２０４Ｂとから構成されている。
【０１１６】
ユーザ端末２０Ｂは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記ＲＯＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末２０Ｂは、その機能を達成する。
【０１１７】
（１）　認証鍵記憶部２０１Ｂ
認証鍵記憶部２０１Ｂは、耐タンパ性を有しており、身元認証指紋情報を記憶する領域を備えている。
（２）　認証部２０２Ｂ
認証部２０２Ｂは、乱数を記憶する乱数記憶領域２５０Ｂを有している。
【０１１８】
認証部２０２Ｂは、カードリーダ３０Ｂより入出力部２０４Ｂを介して、訪問者より入力された指紋から生成された身元認証指紋情報と、カードリーダ３０Ｂに認証カード１０Ｂが挿入されたことを検知した旨を示す検知情報とを受け取ると、受け取った身元認証指紋情報を認証鍵記憶部２０１Ｂへ書き込む。次に、認証部２０２Ｂは、乱数「Ｎ」を生成し、生成した乱数「Ｎ」を入出力部２０４Ｂを介してカードリーダ３０Ｂへ出力し、生成した乱数「Ｎ」を乱数記憶領域２５０Ｂに記憶する。
【０１１９】
さらに、認証部２０２Ｂは、カードリーダ３０Ｂより入出力部２０４Ｂを介して、暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を受け取ると、認証鍵記憶部２０１Ｂにて記憶している身元認証指紋情報を取得して、取得した身元認証指紋情報を用いて、暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）の復号を行い、復号により得られた復号結果と、乱数記憶領域２５０Ｂにて記憶している乱数「Ｎ」とが一致するか否かを判断する。
【０１２０】
復号結果と乱数「Ｎ」とが一致する場合には、認証部２０２Ｂは、カードリーダ３０Ｂに挿入された認証カードが正当な認証カードであると認証し、認証結果として訪問者が正当な訪問者である旨を示す正当訪問者情報を生成し、生成した正当訪問者情報を表示部２０３Ｂへ出力する。復号結果と乱数「Ｎ」とが一致しない場合には、認証部２０２Ｂは、カードリーダ３０Ｂに挿入された認証カードが不正な認証カードであると認証し、認証結果として訪問者が不正な訪問者である旨を示す不正訪問者情報を生成し、生成した不正訪問者情報を表示部２０３Ｂへ出力する。さらに、認証部２０２Ｂは、認証鍵記憶部２０１Ｂにて記憶している身元認証指紋情報、及び乱数記憶領域２５０Ｂにて記憶している乱数「Ｎ」の消去を行う。
【０１２１】

（３）　表示部２０３Ｂ

表示部２０３Ｂは、第２の実施の形態にて示したユーザ端末２０Ａの表示部２０３Ａと同様であるため、説明は省略する。つまり、第１の実施の形態にて示したユーザ端末２０の表示部２０３とも同様である。

（４）　入出力部２０４Ｂ

入出力部２０４Ｂは、第２の実施の形態にて示したユーザ端末２０Ａの入出力部２０４Ａと同様であるため、説明は省略する。つまり、第１の実施の形態にて示したユーザ端末２０の入出力部２０４とも同様である。

【０１２２】

３．４　カードリーダ３０Ｂ

カードリーダ３０Ｂは、図１７に示すように、カード読取部３０１Ｂ、入出力部３０２Ｂ、表示部３０３Ｂ及び指紋読取部３１０Ｂから構成されている。

カードリーダ３０Ｂは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＲＯＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、カードリーダ３０Ｂは、その機能を達成する。

【０１２３】

（１）　カード読取部３０１Ｂ

カード読取部３０１Ｂは、認証カード１０Ｂが挿入されたことの検知を行う。カード読取部３０１Ｂは、認証カード１０Ｂが挿入されたことを検知すると、指紋の入力を要求する要求情報を生成し、生成した要求情報を表示部３０３Ｂへ出力する。次に、カード読取部３０１Ｂは、指紋読取部３１０Ｂより身元認証指紋情報を受け取ると、検知情報を生成し、生成した検知情報と指紋読取部３１０Ｂより受け取った身元認証指紋情報とを入出力部３０２Ｂを介してユーザ端末２０Ｂへ出力する。

【０１２４】

さらに、カード読取部３０１Ｂは、ユーザ端末２０Ｂより入出力部３０２Ｂを介して、乱数「Ｎ」を受け取ると、受け取った乱数「Ｎ」を認証カード１０Ｂへ出力する。カード読取部３０１Ｂは、認証カード１０Ｂより暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を受け取ると、受け取った暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を入出力部３０２Ｂを介してユーザ端末２０Ｂへ出力する。

【０１２５】

（２）　表示部３０３Ｂ

表示部３０３Ｂは、例えば、ディスプレイを備え、カード読取部３０１Ｂより要求情報を受け取ると、受け取った要求情報を表示する。これにより、訪問者へ指紋の入力を促すことができる。

（３）　指紋読取部３１０Ｂ

指紋読取部３１０Ｂは、指紋センサーから構成され、指紋センサーにより、訪問者の指紋模様を読み取り、読み取った指紋模様を用いて、指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報をカード読取部３０１Ｂへ出力する。

【０１２６】

ここで、指紋模様の特徴点とは、隆線の端点や分岐点の方向や位置関係である。

（４）　入出力部３０２Ｂ

入出力部３０２Ｂは、第２の実施の形態にて示したカードリーダ３０Ａの入出力部３０２Ａと同様であるため、説明は省略する。つまり、第１の実施の形態にて示したカードリーダ３０の入出力部３０２とも同様である。

【０１２７】

３．５　身元認証処理の動作

ここでは、認証カード１０Ｂがカードリーダ３０Ｂに挿入されてからユーザ端末２０Ｂにて認証を行うまでの処理である身元認証処理の動作について、図１８に示す流れ図を用いて説明する。

カードリーダ３０Ｂは、認証カード１０Ｂが挿入されたことを検知すると（ステップＳ４００）、要求情報を生成し、生成した要求情報を表示する（ステップＳ４０５）。次にカードリーダ３０Ｂは、訪問者より入力された指紋より身元認証指紋情報を生成し（ステップＳ４１０）、さらに、検知情報を生成し（ステップＳ４１５）、ステップＳ４１０にて生成した身元認証指紋情報と、ステップＳ４１５にて生成した検知情報とをユーザ端末２０Ｂへ出力する（ステップＳ４２０）。

【０１２８】

ユーザ端末２０Ｂは、カードリーダ３０Ｂより身元認証指紋情報と検知情報とを受け取ると、受け取った身元認証指紋情報を認証鍵記憶部２０１Ｂへ書き込む（ステップＳ４２５）。次に、ユーザ端末２０Ｂは、乱数「Ｎ」を生成し、生成した乱数「Ｎ」をカードリーダ３０Ｂへ出力し、さらに、生成した乱数「Ｎ」を乱数記憶領域２５０Ｂに記憶する（ステップＳ４３０）。

【０１２９】

カードリーダ３０Ｂは、ユーザ端末２０Ｂより乱数「Ｎ」を受け取ると、受け取った乱数「Ｎ」を認証カード１０Ｂへ出力する（ステップＳ４３５）。

認証カード１０Ｂは、カードリーダ３０Ｂより乱数「Ｎ」を受け取ると（ステップＳ４４０）、受け取った乱数「Ｎ」を証明鍵記憶部１０１Ｂにて記憶している身元証明鍵を用いて暗号化して、暗号化情報を生成し、生成した暗号化情報をカードリーダ３０Ｂへ出力する（ステップＳ４４５）。

【０１３０】

カードリーダ３０Ｂは、認証カード１０Ｂより暗号化情報を受け取ると、受け取った暗号化情報をユーザ端末２０Ｂへ出力する（ステップＳ４５０）。

ユーザ端末２０Ｂは、カードリーダ３０Ｂより暗号化情報を受け取ると、受け取った暗号化情報と認証鍵記憶部２０１Ｂにて記憶している身元認証指紋情報とを用いて、認証処理を行う（ステップＳ４５５）。

【０１３１】

３．６　認証処理の動作

ここでは、身元認証処理のステップＳ４５５にて行われる認証処理について、図１９に示す流れ図を用いて説明する。

ユーザ端末２０Ｂは、認証カード１０Ｂよりカードリーダ３０Ｂを介して暗号化情報を受け取る（ステップＳ５００）。次に、ユーザ端末２０Ｂは、身元認証指紋情報を認証鍵記憶部２０１Ｂより取得する（ステップＳ５０５）。さらに、ユーザ端末２０Ｂは、取得した身元認証指紋情報を用いて、ステップＳ５００にて受け取った暗号化情報を復号する（ステップＳ５１０）。

【０１３２】

次に、ユーザ端末２０Ｂは、復号して得られた復号結果と、身元認証処理のステップＳ４３０にて乱数記憶領域２５０Ｂに記憶した乱数「Ｎ」とが一致するか否かの判断を行う（ステップＳ５１５）。

一致すると判断する場合には（ステップＳ５１５における「ＹＥＳ」）、正当訪問者情報を生成し、生成した正当訪問者情報を表示し（ステップＳ５２０）、認証鍵記憶部２０１Ｂにて記憶している身元認証指紋情報及び乱数記憶領域２５０Ｂにて記憶している乱数「Ｎ」を消去し（ステップＳ５３０）、処理を終了する。

【０１３３】

一致しないと判断する場合には（ステップＳ５１５における「ＮＯ」）、不正訪問者情報を生成し、生成した不正訪問者情報を表示し（ステップＳ５２５）、認証鍵記憶部２０１Ｂにて記憶している身元認証指紋情報及び乱数記憶領域２５０Ｂに記憶している乱数「Ｎ」を消去し（ステップＳ５３０）、処理を終了する。

４．第４の実施の形態

ここでは、本発明に係る第４の実施の形態としての身元認証システム１Ｃについて説明する。

【０１３４】
身元認証システム１Ｃでは、以下の動作を行う。
訪問者が利用者宅へ訪問する前に、訪問に係る情報を利用者宅のユーザ端末へ送信し、送信した情報と同様の情報を認証カードへ記憶しておく。訪問時に、先ず、身元認証鍵として訪問者の生体科学的特徴を示すバイオメトリックス情報を用いて、認証カードが正当な認証カードであるか否かの認証を行い、正当な認証カードであると判断する場合に、訪問者による訪問が正しいものであるかを判断するために、認証カードにて記憶している訪問に係る情報と事前に送信した情報とが同一であるか否かを判断する。
【０１３５】
４．１　身元認証システム１Ｃの概要
身元認証システム１Ｃは、図２０に示すように、認証カード１０Ｃ、１１Ｃ、・・・、１２Ｃと、ユーザ端末２０Ｃと、カードリーダ３０Ｃと、配信装置５０Ｃとから構成されている。カードリーダ３０Ｃとユーザ端末２０Ｃとは、ケーブル４０Ｃにて接続されている。
【０１３６】
認証カード１０Ｃ、１１Ｃ、・・・、１２Ｃは、訪問業者より利用者宅へ訪問する訪問者一人一人に割り当てられており、割り当てられた訪問者のバイオメトリックス情報を身元証明鍵として予め記憶している。ここで、バイオメトリックス情報は指紋模様の特徴点からなる身元証明指紋情報とする。つまり、認証カード１０Ｃ、１１Ｃ、・・・、１２Ｃには、それぞれ異なる身元証明鍵が記憶されていることになる。
【０１３７】
カードリーダ３０Ｃは、訪問者より指紋の入力を受け付ける指紋読取部３１０Ｃを有している。
ここで、図２０には、図示していないが、ユーザ端末２０Ｃと同様の構成を有するユーザ端末２１Ｃ、・・・、２２Ｃも配信装置５０Ｃとインターネットを介して接続されている。また、ユーザ端末２１Ｃ、・・・、２２Ｃは、カードリーダ３０Ｃと同様の構成を有するカードリーダ３１Ｃ、・・・、３２Ｃとそれぞれ接続されている。
【０１３８】
ここでは、認証カード１０Ｃとユーザ端末２０Ｃとカードリーダ３０Ｃとを用いて、身元認証システム１Ｃの概要について説明する。なお、認証カード１１Ｃ、・・・、１２Ｃは、認証カード１０Ｃと同様であり、ユーザ端末２１Ｃ、・・・、２２Ｃは、ユーザ端末２０Ｃと同様であり、カードリーダ３１Ｃ、・・・、３２Ｃは、カードリーダ３０Ｃと同様であるため、説明は省略する。
【０１３９】
身元認証システム１Ｃでは、訪問業者が利用者宅へ訪問する前に、訪問者による訪問の正当性を検証するために使用する認証用訪問鍵と証明用訪問鍵とを生成し、訪問時間帯を示す時間情報、訪問内容を示す内容情報及び認証用訪問鍵とからなる認証用訪問情報をユーザ端末２０Ｃへインターネットを介して送信する。さらに、身元認証システム１Ｃでは、送信した認証用訪問情報と対応する証明用訪問情報を、認証用訪問情報を送信したユーザ端末と対応付けて認証カード１０Ｃにて記憶する。ここで、証明用訪問情報は、訪問時間帯を示す証明用時間情報、訪問内容を示す証明用内容情報及び証明用訪問鍵からなる情報である。
【０１４０】
身元認証システム１Ｃは、認証カード１０Ｃがカードリーダ３０Ｃに挿入されると、訪問者に対して指紋の入力を要求する。身元認証システム１Ｃは、カードリーダ３０Ｃの指紋読取部３１０Ｃより指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報と認証カード１０Ｃに記憶している身元証明鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行う。ここで用いる暗号処理は、身元認証システム１と同様に秘密鍵による暗号処理である。また、身元認証システム１と同様に身元証明鍵と身元認証指紋情報とが同一の鍵と

なることは、言うまでもない。

【０１４１】

次に、身元認証システム１Ｃは、カードリーダ３０Ｃに挿入された認証カードが正当な認証カードであると認証した場合には、証明用訪問情報の正当性を検証するために、認証用訪問鍵及び証明用訪問鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行う。ここで用いる暗号処理は、秘密鍵による暗号処理であり、証明用訪問鍵と認証用訪問鍵とが同一の鍵となることは、言うまでもない。

【０１４２】

身元認証システム１Ｃは、上記認証にて、証明用訪問情報が正当であると認証した場合には、認証カード１０Ｃにて記憶されている証明用訪問情報に含まれる訪問時間帯及び訪問内容と、事前に送信された認証用訪問情報に含まれる訪問時間帯及び訪問内容とがそれぞれ一致するか否かを判断し、判断結果をユーザ端末２０Ｃの表示部２０３Ｃにて表示する。

【０１４３】

４．２　配信装置５０Ｃ

配信装置５０Ｃは、訪問者が利用者宅へ訪問する前に、認証用訪問情報をユーザ端末２０Ｃへ送信する装置であり、認証用訪問情報を送信する際には、訪問者に対応する認証カード１０Ｃが配信装置５０Ｃに装着されている。

配信装置５０Ｃは、図２１に示すように、端末情報記憶部５０６Ｃ、制御部５０２Ｃ、操作部５０３Ｃ、送信部５０４Ｃ及び出力部５０５Ｃから構成されている。

【０１４４】

配信装置５０Ｃは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、モデムなどからなどから構成されるコンピュータシステムである。前記ＲＯＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、配信装置５０Ｃは、その機能を達成する。

【０１４５】

（１）　端末情報記憶部５０６Ｃ

端末情報記憶部５０６Ｃは、耐タンパ性を有しており、利用者宅へ配布したユーザ端末を一意に識別する端末ＩＤを記憶している。

なお、ここで記憶されている端末ＩＤの個数は、配布したユーザ端末の数と同一となることは言うまでもない。

【０１４６】

（２）　制御部５０２Ｃ

制御部５０２Ｃは、操作部５０３Ｃより認証用訪問情報をユーザ端末２０Ｃへ配信する旨の訪問用配信情報と、訪問時間帯及び訪問内容とを受け取ると、認証用訪問鍵及び証明用訪問鍵を生成する。さらに制御部５０２Ｃは、生成した認証用訪問鍵、受け取った訪問時間帯及び訪問内容を用いて認証用訪問情報を生成し、生成した認証用訪問情報をユーザ端末２０Ｃへ送信する。また、制御部５０２Ｃは、受け取った訪問時間帯及び訪問内容及び生成した証明用訪問鍵とを用いて証明用訪問情報を生成する。さらに、制御部５０２Ｃは、ユーザ端末２０Ｃを識別する端末ＩＤを端末情報記憶部５０６Ｃより取得し、取得した端末ＩＤと生成した証明用訪問情報とを対応付けて、出力部５０５Ｃを介して認証カード１０Ｃへ出力する。

【０１４７】

（３）　操作部５０３Ｃ

操作部５０３Ｃは、操作者の操作により、訪問用配信情報と、訪問時間帯及び訪問内容とを受け付けると、受け付けた訪問用配信情報と訪問時間帯と訪問内容とを制御部５０２Ｃへ出力する。

なお、操作者は、利用者宅へ訪問する訪問者自身に限らず、訪問業者に属する者であればよい。

【０１４８】
（４）　送信部５０４Ｃ
送信部５０４Ｃは、制御部５０２Ｃより受け取った情報をユーザ端末２０Ｃへインターネットを介して出力する。
（５）　出力部５０５Ｃ
出力部５０５Ｃは、制御部５０２Ｃより受け取った情報を認証カード１０Ｃへ出力する。

【０１４９】
４．３　認証カード１０Ｃ
ここでは、認証カード１０Ｃの構成について説明する。認証カード１０Ｃは、ＩＣを内蔵している可搬型の記録媒体であり、一例として、ＩＣカード機能付メモリカードである。認証カード１０Ｃは、図２２に示すように、証明鍵記憶部１０１Ｃ、訪問鍵記憶部１０５Ｃ、制御部１０２Ｃ及び入出力部１０３Ｃから構成されている。

【０１５０】
認証カード１０Ｃは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＲＯＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード１０Ｃは、その機能を達成する。
なお、認証カード１１Ｃ、・・・、１２Ｃは、認証カード１０Ｃと同様の構成を有しているため、説明は省略する。

【０１５１】
（１）　証明鍵記憶部１０１Ｃ
証明鍵記憶部１０１Ｃは、耐タンパ性を有しており、訪問者に対応する身元証明指紋情報を身元証明鍵として１つ記憶している。
以降の説明において、必要に応じて、身元証明鍵として「ＳＫ１」を用いて説明する。
（２）　訪問鍵記憶部１０５Ｃ
訪問鍵記憶部１０５Ｃは、耐タンパ性を有しており、図２３に一例として示すように、証明用訪問情報テーブルＴ３００を備えている。

【０１５２】
証明用訪問情報テーブルＴ３００は、端末ＩＤ、証明用時間情報、証明用内容情報及び証明用訪問鍵からなる組を１以上記憶するための領域を備えている。
端末ＩＤは、利用者宅に配布したユーザ端末を識別する識別子である。例えば、端末ＩＤ「Ｔ－ＩＤ１」は、ユーザ端末２０Ｃを示し、端末ＩＤ「Ｔ－ＩＤ２」は、ユーザ端末２１Ｃ（図２０では図示せず）を示している。

【０１５３】
証明用時間情報は、訪問者が訪問する時間帯を示す情報であり、証明用内容情報は、訪問内容を示す情報であり、証明用訪問鍵は、訪問者による訪問の正当性を検証するために使用する鍵である。
（３）　制御部１０２Ｃ
制御部１０２Ｃは、配信装置５０Ｃより入出力部１０３Ｃを介して端末ＩＤと証明用訪問情報とを受け取ると、受け取った端末ＩＤと証明用訪問情報とを訪問鍵記憶部１０５Ｃへ書き込む。

【０１５４】
また、制御部１０２Ｃは、カードリーダ３０Ｃより入出力部１０３Ｃを介して、第１乱数「Ｎ１」を受け取ると、証明鍵記憶部１０１Ｃより身元証明鍵「ＳＫ１」を取得し、取得した身元証明鍵「ＳＫ１」を用いて、カードリーダ３０Ｃより受け取った第１乱数「Ｎ１」に対して暗号化を施し、第１暗号化情報Ｅｎｃ（ＳＫ１、Ｎ１）を生成する。制御部１０２Ｃは、生成した暗号化情報を入出力部１０３Ｃを介してカードリーダ３０Ｃへ出力する。

【０１５５】

さらに、制御部１０２Ｃは、カードリーダ３０Ｃより入出力部１０３Ｃを介して端末ＩＤと第２乱数「Ｎ２」とを受け取ると、受け取った端末ＩＤに対応する証明用訪問情報を取得し、取得した証明用訪問鍵を一時的に記憶する。

また、制御部１０２Ｃは、取得した証明用訪問情報に含まれる証明用訪問鍵「Ｖ－Ｋｅｙ１」を取得し、取得した証明用訪問鍵「Ｖ－Ｋｅｙ１」を用いて、カードリーダ３０Ｃより受け取った第２乱数「Ｎ２」に対して暗号化を施し、第２暗号化情報Ｅｎｃ（Ｖ－Ｋｅｙ１、Ｎ２）を生成する。制御部１０２Ｃは、生成した第２暗号化情報を入出力部１０３Ｃを介してカードリーダ３０Ｃへ出力する。

【０１５６】

さらに、制御部１０２Ｃは、証明用訪問情報に含まれる証明用時間情報と証明用内容情報をユーザ端末２０Ｃへ出力する旨を示す出力指示情報をカードリーダ３０Ｃより受け取ると、一時的に記憶している証明用訪問情報に含まれる証明用時間情報と証明用内容情報とを取得し、取得した証明用時間情報と証明用内容情報とを入出力部１０３Ｃを介してカードリーダ３０Ｃへ出力する。

【０１５７】

（４）　入出力部１０３Ｃ

入出力部１０３Ｃは、第３の実施の形態にて示した認証カード１０Ｂの入出力部１０３Ｂと同様であるため、説明は省略する。つまり、入出力部１０３Ｃは、第１の実施の形態にて示した認証カード１０の入出力部１０３、及び第２の実施の形態にて示した認証カード１０Ａの入出力部１０３Ａとも同様である。

【０１５８】

４．４　ユーザ端末２０Ｃの構成

ここでは、ユーザ端末２０Ｃの構成について説明する。ユーザ端末２０Ｃは、図２４に示すように、認証鍵記憶部２０１Ｃ、認証部２０２Ｃ、表示部２０３Ｃ、入出力部２０４Ｃ、受信部２０５Ｃ、訪問情報記憶部２０６Ｃ及び時計部２０７Ｃとから構成されている。

【０１５９】

ユーザ端末２０Ｃは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記ＲＯＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末２０Ｃは、その機能を達成する。

【０１６０】

また、上記の身元認証システム１Ｃの概要にて示したように、ユーザ端末２１Ｃ、・・・、２２Ｃは、ユーザ端末２０Ｃと同様の構成であるため、説明は省略する。

（１）　認証鍵記憶部２０１Ｃ

認証鍵記憶部２０１Ｃは、第３の実施の形態にて示したユーザ端末２０Ｂの認証鍵記憶部２０１Ｂと同様であるため、説明は省略する。

【０１６１】

（２）　訪問情報記憶部２０６Ｃ

訪問情報記憶部２０６Ｃは、耐タンパ性を有しており、配信装置５０Ｃより送信された認証用訪問情報を記憶する領域を備えている。

（３）　受信部２０５Ｃ

受信部２０５Ｃは、配信装置５０Ｃよりインターネットを介して、認証用訪問情報を受信すると、受信した認証用訪問情報を訪問情報記憶部２０６Ｃへ書き込む。

【０１６２】

これにより、ユーザ端末２０Ｃは、訪問業者による訪問に係る情報を事前に記憶することができる。

（４）　時計部２０７Ｃ

時計部２０７Ｃは、時刻を計時する。

（５）　認証部２０２Ｃ

認証部２０２Ｃは、乱数を記憶する乱数記憶領域２５０Ｃを有しており、さらに、ユーザ端末２０Ｃの端末ＩＤをも予め記憶している。

【０１６３】

認証部２０２Ｃは、カードリーダ３０Ｃより入出力部２０４Ｃを介して、訪問者より入力された指紋から生成された身元認証指紋情報と、カードリーダ３０Ｃに認証カード１０Ｃが挿入されたことを検知した旨を示す検知情報とを受け取ると、受け取った身元認証指紋情報を認証鍵記憶部２０１Ｃへ書き込む。次に、認証部２０２Ｃは、第１乱数「Ｎ１」を生成し、生成した第１乱数「Ｎ１」を入出力部２０４Ｃを介してカードリーダ３０Ｃへ出力し、生成した第１乱数「Ｎ１」を乱数記憶領域２５０Ｃに記憶する。

【０１６４】

さらに、認証部２０２Ｃは、カードリーダ３０Ｃより入出力部２０４Ｃを介して、第１暗号化情報Ｅｎｃ（ＳＫ１、Ｎ１）を受け取ると、認証鍵記憶部２０１Ｃにて記憶している身元認証指紋情報を取得し、取得した身元認証指紋情報を用いて、第１暗号化情報Ｅｎｃ（ＳＫ１、Ｎ１）の復号を行い、復号により得られた復号結果と、乱数記憶領域２５０Ｃにて記憶している第１乱数「Ｎ１」とが一致するか否かを判断する。

【０１６５】

復号結果と第１乱数「Ｎ１」とが一致しない場合には、認証部２０２Ｃは、カードリーダ３０Ｃに挿入された認証カードが不正な認証カードであると認証し、認証結果として不正訪問者情報を生成し、生成した不正訪問者情報を表示部２０３Ｃへ出力する。さらに、認証部２０２Ｃは、認証鍵記憶部２０１Ｃにて記憶している身元認証指紋情報及び乱数記憶領域２５０Ｃにて記憶している第１乱数「Ｎ１」の消去を行う。

【０１６６】

復号結果と第１乱数「Ｎ１」とが一致する場合には、認証部２０２Ｃは、予め記憶している端末ＩＤを取得し、さらに、第２乱数「Ｎ２」を生成し、乱数記憶領域２５０Ｃに記憶している内容を第１乱数「Ｎ１」から生成した第２乱数「Ｎ２」へと更新する。次に、認証部２０２Ｃは、生成した第２乱数「Ｎ２」と取得した端末ＩＤとを入出力部２０４Ｃを介してカードリーダ３０Ｃへ出力する。さらに、認証部２０２Ｃは、カードリーダ３０Ｃより入出力部２０４Ｃを介して、第２暗号化情報Ｅｎｃ（Ｖ－Ｋｅｙ１、Ｎ２）を受け取ると、訪問情報記憶部２０６Ｃにて記憶している認証用訪問情報を取得する。認証部２０２Ｃは、受け取った第２暗号化情報Ｅｎｃ（Ｖ－Ｋｅｙ１、Ｎ２）を、取得した認証用訪問情報に含まれる認証用訪問鍵を用いて、第２暗号化情報Ｅｎｃ（Ｖ－Ｋｅｙ１、Ｎ２）の復号を行い、復号により得られた復号結果と、乱数記憶領域２５０Ｃにて記憶している第２乱数「Ｎ２」とが一致するか否かを判断する。

【０１６７】

一致しない場合には、認証部２０２Ｃは、カードリーダ３０Ｃに挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示部２０３Ｃへ出力し、乱数記憶領域２５０Ｃにて記憶している第２乱数「Ｎ２」を消去する。

一致する場合には、出力指示情報を生成し、生成した出力指示情報を入出力部２０４Ｃを介してカードリーダ３０Ｃへ出力する。さらに、認証部２０２Ｃは、カードリーダ３０Ｃより入出力部２０４Ｃを介して、証明用時間情報と証明用内容情報とを受け取ると、次の動作を行う。認証部２０２Ｃは、訪問情報記憶部２０６Ｃにて記憶している認証用訪問情報を取得する。次に、受け取った証明用時間情報及び証明用内容情報と、取得した認証用訪問情報に含まれる時間情報及び内容情報とがそれぞれ一致するか否かの判断を行う。

【０１６８】

少なくとも何れかが一致しない場合には、認証部２０２Ｃは、カードリーダ３０Ｃに挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示部２０３Ｃへ出力する。

それぞれが一致すると判断する場合には、時計部２０７Ｃより現在時刻を取得し、取得

した現在時刻が認証用時間情報にて示される訪問時間帯の範囲であるか否かを判断する。訪問時間帯の範囲でないと判断する場合には、認証部２０２Ｃは、カードリーダ３０Ｃに挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示部２０３Ｃへ出力し、訪問情報記憶部２０６Ｃにて記憶している認証用訪問情報、及び乱数記憶領域２５０Ｃにて記憶している第２乱数「Ｎ２」を消去する。

【０１６９】

訪問時間帯の範囲であると判断する場合には、認証部２０２Ｃは、正当訪問者情報を生成し、生成した正当訪問者情報を表示部２０３Ｃへ出力し、訪問情報記憶部２０６Ｃにて記憶している認証用訪問情報、及び乱数記憶領域２５０Ｃにて記憶している第２乱数「Ｎ２」を消去する。

（６）　表示部２０３Ｃ

表示部２０３Ｃは、第３の実施の形態にて示したユーザ端末２０Ｂの表示部２０３Ｂと同様であるため、説明は省略する。つまり、第１の実施の形態にて示したユーザ端末２０の表示部２０３、及び第２の実施の形態にて示したユーザ端末２０Ａの表示部２０３Ａとも同様である。

【０１７０】

（７）　入出力部２０４Ｃ

入出力部２０４Ｃは、第３の実施の形態にて示したユーザ端末２０Ｂの入出力部２０４Ｂと同様であるため、説明は省略する。つまり、第１の実施の形態にて示したユーザ端末２０の入出力部２０４、及び第２の実施の形態にて示したユーザ端末２０Ａの入出力部２０４Ａとも同様である。

【０１７１】

４．５　カードリーダ３０Ｃ

カードリーダ３０Ｃは、図２４に示すように、カード読取部３０１Ｃ、入出力部３０２Ｃ、表示部３０３Ｃ及び指紋読取部３１０Ｃから構成されている。

カードリーダ３０Ｃは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＲＯＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、カードリーダ３０Ｃは、その機能を達成する。

【０１７２】

なお、上記の身元認証システム１Ｃの概要にて示したように、カードリーダ３１Ｃ、・・・、３２Ｃは、カードリーダ３０Ｃと同様の構成であるため、説明は省略する。

（１）　カード読取部３０１Ｃ

カード読取部３０１Ｃは、認証カード１０Ｃが挿入されたことの検知を行う。カード読取部３０１Ｃは、認証カード１０Ｃが挿入されたことを検知すると、指紋の入力を要求する要求情報を生成し、生成した要求情報を表示部３０３Ｃへ出力する。次に、カード読取部３０１Ｃは、指紋読取部３１０Ｃより身元認証指紋情報を受け取ると、検知情報を生成し、生成した検知情報と指紋読取部３１０Ｃより受け取った身元認証指紋情報とを入出力部３０２Ｃを介してユーザ端末２０Ｃへ出力する。

【０１７３】

カード読取部３０１Ｃは、ユーザ端末２０Ｃより入出力部３０２Ｃを介して、第１乱数「Ｎ１」を受け取ると、受け取った第１乱数「Ｎ１」を認証カード１０Ｃへ出力する。カード読取部３０１Ｃは、認証カード１０Ｃより第１暗号化情報Ｅｎｃ（ＳＫ１、Ｎ１）を受け取ると、受け取った第１暗号化情報Ｅｎｃ（ＳＫ１、Ｎ１）を入出力部３０２Ｃを介してユーザ端末２０Ｃへ出力する。

【０１７４】

カード読取部３０１Ｃは、入出力部３０２Ｃを介してユーザ端末２０Ｃより端末ＩＤと第２乱数「Ｎ２」とを受け取ると、受け取った端末ＩＤと第２乱数「Ｎ２」とを認証カード１０Ｃへ出力する。さらに、カード読取部３０１Ｃは、認証カード１０Ｃより第２暗号

化情報Ｅｎｃ（Ｖ－Ｋｅｙ１、Ｎ２）を受け取ると、受け取った第２暗号化情報Ｅｎｃ（Ｖ－Ｋｅｙ１、Ｎ２）を入出力部３０２Ｃを介してユーザ端末２０Ｃへ出力する。

【０１７５】

カード読取部３０１Ｃは、入出力部３０２Ｃを介してユーザ端末２０Ｃより出力指示情報を受け取ると、受け取った出力指示情報を認証カード１０Ｃへ出力する。さらに、カード読取部３０１Ｃは、認証カード１０Ｃより認証用時間情報及び認証用内容情報を受け取ると、受け取った認証用時間情報及び認証用内容情報を入出力部３０２Ｃを介してユーザ端末２０Ｃへ出力する。

【０１７６】

（２）　表示部３０３Ｃ

表示部３０３Ｃは、第３の実施の形態で示したカードリーダ３０Ｂの表示部３０３Ｂと同様であるため、説明は省略する。

（３）　指紋読取部３１０Ｃ

指紋読取部３１０Ｃは、第３の実施の形態で示したカードリーダ３０Ｂの指紋読取部３１０Ｂと同様であるため、説明は省略する。

【０１７７】

（４）　入出力部３０２Ｃ

入出力部３０２Ｃは、第３の実施の形態にて示したカードリーダ３０Ｂの入出力部３０２Ｂと同様であるため、説明は省略する。つまり、第１の実施の形態にて示したカードリーダ３０の入出力部３０２、及び第２の実施の形態にて示したカードリーダ３０Ａの入出力部３０２Ａとも同様である。

【０１７８】

４．６　訪問情報配信処理の動作

ここでは、認証用訪問情報を事前に配信する訪問情報配信処理について、図２５に示す流れ図を用いて、説明する。

配信装置５０Ｃは、利用者の操作により、認証用訪問情報をユーザ端末２０Ｃへ配信する旨の訪問用配信情報と、訪問時間帯及び訪問内容とを受け付けると（ステップＳ６００）、認証用訪問鍵及び証明用訪問鍵とを生成する（ステップＳ６０５）。次に、配信装置５０Ｃは、生成した認証用訪問鍵と、ステップＳ６００にて受け取った訪問時間帯及び訪問内容とを用いて認証用訪問情報を生成し、生成した認証用訪問情報をユーザ端末２０Ｃへ送信する（ステップＳ６１０）。ユーザ端末２０Ｃは、配信装置５０Ｃより認証用訪問情報を受信すると（ステップＳ６１５）、受信した認証用訪問情報を訪問情報記憶部２０６Ｃへ書き込む（ステップＳ６２０）。

【０１７９】

配信装置５０Ｃは、さらに、ステップＳ６０５にて生成した証明用訪問鍵と、ステップＳ６００にて受け取った訪問時間帯及び訪問内容とを用いて証明用訪問情報を生成し、生成した証明用訪問情報を認証カード１０Ｃへ出力する（ステップＳ６２５）。

認証カード１０Ｃは、証明用訪問情報を受け取ると、受け取った証明用訪問情報を訪問鍵記憶部１０５Ｃへ書き込む（ステップＳ６３０）。

【０１８０】

４．７　身元認証処理の動作

ここでは、カードリーダ３０Ｃに挿入された認証カード１０Ｃの認証を行う処理である身元認証処理の動作について、図２６及び図２７に示す流れ図を用いて、説明する。

カードリーダ３０Ｃは、認証カード１０Ｃが挿入されたことを検知すると（ステップＳ６５０）、要求情報を生成し、生成した要求情報を表示する（ステップＳ６５５）。次に、カードリーダ３０Ｃは、訪問者より入力された指紋より身元認証指紋情報を生成し（ステップＳ６６０）、さらに、検知情報を生成し（ステップＳ６６５）、ステップＳ６６０にて生成した身元認証指紋情報と、ステップＳ６６５にて生成した検知情報とをユーザ端末２０Ｃへ出力する（ステップＳ６７０）。

【０１８１】

ユーザ端末２０Ｃは、カードリーダ３０Ｃより身元認証指紋情報と検知情報とを受け取ると、受け取った身元認証指紋情報を認証鍵記憶部２０１Ｃへ書き込む（ステップＳ６７５）。次に、ユーザ端末２０Ｃは、第１乱数「Ｎ１」を生成し、生成した第１乱数「Ｎ１」をカードリーダ３０Ｃへ出力し、さらに、生成した第１乱数「Ｎ１」を乱数記憶領域２５０Ｃに記憶する（ステップＳ６８０）。

【０１８２】

カードリーダ３０Ｃは、ユーザ端末２０Ｃより第１乱数「Ｎ１」を受け取ると、受け取った第１乱数「Ｎ１」を認証カード１０Ｃへ出力する（ステップＳ６８５）。

認証カード１０Ｃは、カードリーダ３０Ｃより第１乱数「Ｎ１」を受け取ると（ステップＳ６９０）、受け取った第１乱数「Ｎ１」を証明鍵記憶部１０１Ｃにて記憶している身元証明鍵を用いて暗号化して、第１暗号化情報を生成し、生成した第１暗号化情報をカードリーダ３０Ｃへ出力する（ステップＳ６９５）。

【０１８３】

カードリーダ３０Ｃは、認証カード１０Ｃより第１暗号化情報を受け取ると、受け取った第１暗号化情報をユーザ端末２０Ｃへ出力する（ステップＳ７００）。

ユーザ端末２０Ｃは、カードリーダ３０Ｃより第１暗号化情報を受け取ると、受け取った第１暗号化情報と認証鍵記憶部２０１Ｃにて記憶している身元認証指紋情報とを用いて、認証処理を行う（ステップＳ７０５）。

【０１８４】

ユーザ端末２０Ｃは、認証処理にて、カードリーダに挿入された認証カードが正当な認証カードであると判断すると、端末ＩＤを取得し（ステップＳ７１０）、さらに、第２乱数「Ｎ２」を生成し、乱数記憶領域２５０Ｃに記憶している内容を第１乱数「Ｎ１」から生成した第２乱数「Ｎ２」へと更新する（ステップＳ７１５）。次に、ユーザ端末２０Ｃは、取得した端末ＩＤと生成した第２乱数「Ｎ２」とをカードリーダ３０Ｃへ出力する（ステップＳ７２０）。

【０１８５】

カードリーダ３０Ｃは、ユーザ端末２０Ｃより端末ＩＤと第２乱数「Ｎ２」とを受け取ると、受け取った端末ＩＤと第２乱数「Ｎ２」とを認証カード１０Ｃへ出力する（ステップＳ７２５）。

認証カード１０Ｃは、カードリーダ３０Ｃより端末ＩＤと第２乱数「Ｎ２」とを受け取ると（ステップＳ７３０）、受け取った端末ＩＤに対応する証明用訪問情報を取得し、取得した証明用訪問情報を一時的に記憶する（ステップＳ７３５）。次に、認証カード１０Ｃは、取得した証明用訪問情報に含まれる証明用訪問鍵を用いて暗号化して、第２暗号化情報を生成し、生成した第２暗号化情報をカードリーダ３０Ｃへ出力する（ステップＳ７４０）。

【０１８６】

カードリーダ３０Ｃは、認証カード１０Ｃより第２暗号化情報を受け取ると、受け取った第２暗号化情報をユーザ端末２０Ｃへ出力する（ステップＳ７４５）。

ユーザ端末２０Ｃは、カードリーダ３０Ｃより第２暗号化情報を受け取ると、受け取った第２暗号化情報と訪問情報記憶部２０６Ｃにて記憶している認証用訪問情報に含まれる認証用訪問鍵とを用いて、訪問鍵認証処理を行う（ステップＳ７５０）。

【０１８７】

ユーザ端末２０Ｃは、訪問鍵認証証処理にて、認証カード１０Ｃに記憶されている証明用訪問情報が正当であると判断すると、出力指示情報を生成し、生成した出力指示情報をカードリーダ３０Ｃへ出力する（ステップＳ７５５）。

カードリーダ３０Ｃは、ユーザ端末２０Ｃより出力指示情報を受け取ると、受け取った出力指示情報を認証カードへ出力する（ステップＳ７６０）。

【０１８８】

認証カード１０Ｃは、カードリーダ３０Ｃより出力指示情報を受け取ると、一時的に記憶している証明用訪問情報に含まれる証明用時間情報及び証明用内容情報を取得し、取得

した証明用時間情報及び証明用内容情報をカードリーダ３０Ｃへ出力する（ステップＳ７６５）。

カードリーダ３０Ｃは、認証カード１０Ｃより証明用時間情報及び証明用内容情報を受け取ると、受け取った証明用時間情報及び証明用内容情報をユーザ端末２０Ｃへ出力する（ステップＳ７７０）。

【０１８９】

ユーザ端末２０Ｃは、カードリーダ３０Ｃより証明用時間情報及び証明用内容情報を受け取ると、受け取った証明用時間情報及び証明用内容情報と、訪問情報記憶部２０６Ｃにて記憶している認証用訪問情報とを用いて、訪問情報検証処理を行う（ステップＳ７７５）。

４．８　認証処理

図２６にて示した身元認証処理のステップＳ７０５にて行われる認証処理について、図１９にて示した認証処理との変更点を中心に説明する。

【０１９０】

先ず、ステップＳ５１５にて、肯定的に判断する場合（ステップＳ５１５における「ＹＥＳ」）、ステップＳ５２０以降は行わないで、図２７に示すステップＳ７１０以降を行うように変更する。否定的に判断する場合は（ステップＳ５１５における「ＮＯ」）、図１９に示す動作と同様である。なお、図２７にて示す認証処理では、図１９に示す乱数及び暗号化情報を、第１乱数及び第１暗号化情報と読み替える。

【０１９１】

４．９　訪問鍵認証処理

ここでは、図２７にて示した身元認証処理のステップＳ７５０にて行われる訪問鍵認証処理について、図２８に示す流れ図を用いて説明する。

ユーザ端末２０Ｃは、認証カード１０Ｃよりカードリーダ３０Ｃを介して、第２暗号化情報を受け取る（ステップＳ８００）。次に、ユーザ端末２０Ｃは、訪問情報記憶部２０６Ｃにて記憶している認証用訪問情報を取得し（ステップＳ８０５）、取得した認証用訪問情報に含まれる認証用訪問鍵を用いて、第２暗号化情報の復号を行い（ステップＳ８１０）、復号により得られた復号結果と、乱数記憶領域２５０Ｃにて記憶している第２乱数「Ｎ２」とが一致するか否かを判断する（ステップＳ８１５）。

【０１９２】

一致すると判断する場合には（ステップＳ８１５における「ＹＥＳ」）、図２７にて示すステップＳ７５５以降を行う。

一致しないと判断する場合には（ステップＳ８１５における「ＮＯ」）、不正訪問者情報を生成し、生成した不正訪問者情報を表示部２０３Ｃへ出力し、乱数記憶領域２５０Ｃにて記憶している第２乱数「Ｎ２」を消去する（ステップＳ８２０）。

【０１９３】

４．１０　訪問情報検証処理

ここでは、図２７にて示した身元認証処理のステップＳ７７５にて行われる訪問情報検証処理について、図２９に示す流れ図を用いて説明する。

ユーザ端末２０Ｃは、認証カード１０Ｃよりカードリーダ３０Ｃを介して、証明用時間情報及び証明用内容情報とを受け取る（ステップＳ８５０）。次に、ユーザ端末２０Ｃは、訪問情報記憶部２０６Ｃにて記憶している認証用訪問情報を取得する（ステップＳ８５５）。

【０１９４】

ユーザ端末２０Ｃは、取得した認証用訪問情報に含まれる認証用時間情報と証明用時間情報とが一致するか否かの判断、つまり事前に受信した訪問時間帯と認証カード１０Ｃに記憶されている訪問時間帯とが一致するか否かの判断をする（ステップＳ８６０）。

時間帯が一致すると判断する場合には（ステップＳ８６０における「ＹＥＳ」）、取得した認証用訪問情報に含まれる認証用内容情報と証明用内容情報とが一致するか否かの判断、つまり事前に受信した訪問内容と認証カード１０Ｃに記憶されている訪問内容とが一

致するか否かの判断をする（ステップＳ８６５）。

【０１９５】

訪問内容が一致すると判断する場合には（ステップＳ８６５における「ＹＥＳ」）、時計部２０７Ｃより現在の時刻を取得し（ステップＳ８７０）、取得した現在時刻が、認証用時間情報に示される時間帯の範囲内であるか否かを判断する（ステップＳ８７５）。

取得した現在時刻が、認証用時間情報に示される時間帯の範囲内であると判断する場合には（ステップＳ８７５における「ＹＥＳ」）、正当訪問者情報を生成し、生成した正当訪問者情報を表示し（ステップＳ８８０）、訪問情報記憶部２０６Ｃにて記憶している認証用訪問情報、及び乱数記憶領域２５０Ｃにて記憶している第２乱数「Ｎ２」を消去する（ステップＳ８９０）。

【０１９６】

時間帯が一致しないと判断する場合（ステップＳ８６０における「ＮＯ」）、訪問内容が一致しないと判断する場合（ステップＳ８６５における「ＮＯ」）、及び取得した現在時刻が認証用時間情報に示される時間帯の範囲内でないと判断する場合（ステップＳ８７５における「ＮＯ」）のうち何れかの場合には、不正訪問者情報を生成し、生成した不正訪問者情報を表示し、訪問情報記憶部２０６Ｃにて記憶している認証用訪問情報、及び乱数記憶領域２５０Ｃにて記憶している第２乱数「Ｎ２」を消去する（ステップＳ８９０）。

【０１９７】

５．まとめ

以上、説明したように、本発明によれば、身元認証システムは、認証カードとユーザ端末との間で認証を行っている。そのため、従来のようにネットワーク接続されたサーバを用いて認証を行う必要がない。つまり、ユーザ端末とサーバとが通信できないため、訪問者の身分の確認ができなくなるという問題は生じなくなる。

【０１９８】

また、認証を行う毎に、乱数を発生させているため、認証カードにて生成される暗号化情報は、認証を行う毎に異なる内容となる。そのため、通信経路盗聴による成りすまし攻撃に対する耐性が高くなる。

また、身元認証鍵を配信する場合には、利用者宅の訪問前に任意のタイミングで身元認証鍵を配信することができるため、身元認証鍵の配信によるネットワーク負荷を避けることができる。つまり、複数の利用者宅へ身元認証鍵を配信する際に、分散させて配信することが可能となる。

【０１９９】

（変形例）

上記に説明した第１、第２、第３及び第４の実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

（１）上記第１、第２、第３及び第４の実施の形態にて示した認証処理において、チャレンジレスポンス方式による認証方法として、秘密鍵暗号処理を用いたが、これに限定されない。他の暗号処理を用いたチャレンジレスポンス方式による認証方法でもよい。

【０２００】

例えば、公開鍵暗号処理を用いたチャレンジレスポンス方式による認証、認証を行う毎に異なる電子署名を用いたチャレンジレスポンス方式による認証、固定の電子署名を用いたチャレンジレスポンス方式による認証などである。

（ａ）公開鍵暗号処理を用いる場合

ここでは、各実施の形態ごとに、公開鍵暗号処理を用いた場合の変形例について説明する。

【０２０１】

＜第１の実施の形態の変形例＞

公開鍵暗号処理を用いた場合の身元認証システムについて、第１の実施の形態と異なる

点を中心に説明する。ここで、公開鍵暗号処理は、一例として、ＲＳＡである。ＲＳＡについては、公知であるため、説明は省略する。

認証カード１０は、身元証明鍵「ＳＫ１」を秘密鍵として、証明鍵ＩＤと対応付けて記憶している。

【０２０２】

ユーザ端末２０は、公開鍵である身元認証鍵と、身元認証鍵を識別する認証鍵ＩＤとからなる組を複数記憶している。なお、以降では、身元証明鍵「ＳＫ１」に対応する公開鍵である身元認証鍵を「ＰＫ１」として説明を行う。

ユーザ端末２０は、カードリーダ３０より検知情報と証明鍵ＩＤとを受け取ると、証明ＩＤと一致する認証ＩＤに対応付けられた身元認証鍵「ＰＫ１」を取得する。次に、ユーザ端末２０は、乱数「Ｎ」を生成し、生成した乱数「Ｎ」を乱数記憶領域２５０に記憶し、さらに、生成した乱数「Ｎ」を取得した身元認証鍵「ＰＫ１」を用いて暗号化を行い、暗号化情報Ｅｎｃ（ＰＫ１、Ｎ）を生成し、生成した暗号化情報Ｅｎｃ（ＰＫ１、Ｎ）をカードリーダ３０を介して認証カード１０へ出力する。

【０２０３】

認証カード１０は、ユーザ端末２０より暗号化情報Ｅｎｃ（ＰＫ１、Ｎ）を受け取ると、受け取った暗号化情報Ｅｎｃ（ＰＫ１、Ｎ）を、記憶している身元証明鍵「ＳＫ１」を用いて、復号を行い、復号にて得られた復号結果をカードリーダ３０を介してユーザ端末２０へ出力する。

ユーザ端末２０は、認証カード１０より復号結果を受け取ると、受け取った復号結果と、記憶している乱数「Ｎ」とが一致するか否かを判断を行い、一致すると判断する場合には、カードリーダ３０Ａに挿入された認証カードが正当な認証カードであると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。一致しないと判断する場合には、カードリーダ３０に挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。次に、ユーザ端末２０は、乱数記憶領域２５０にて記憶している情報及びデータを消去する。

【０２０４】

＜第２の実施の形態の変形例＞

第２の実施の形態と異なる点を中心に説明する。認証カード１０Ａは、秘密鍵として身元証明鍵「ＳＫ１」を認証鍵記憶部２０１Ａにて記憶している。また、ユーザ端末２０Ａは、事前に配信装置５０Ａより配信された公開鍵である身元認証鍵「ＰＫ１」を記憶している。認証時の動作について、以下に説明する。ユーザ端末２０Ａは、カードリーダ３０Ａより検知情報を受け取ると、身元認証鍵「ＰＫ１」を認証鍵記憶部２０１Ａより取得する。次に、ユーザ端末２０Ａは、乱数「Ｎ」を生成し、生成した乱数「Ｎ」を乱数記憶領域２５０Ａに記憶し、さらに、生成した乱数「Ｎ」を取得した身元認証鍵「ＰＫ１」を用いて暗号化を行い、暗号化情報Ｅｎｃ（ＰＫ１、Ｎ）を生成し、生成した暗号化情報Ｅｎｃ（ＰＫ１、Ｎ）をカードリーダ３０Ａを介して認証カード１０Ａへ出力する。以降は、上記で示した動作と同様であるため、説明は省略する。なお、認証処理の終了時は、乱数記憶領域２５０Ａにて記憶している乱数「Ｎ」の消去及び認証鍵記憶部２０１Ａにて記憶している身元認証鍵「ＰＫ１」の消去を行う。

【０２０５】

＜第３の実施の形態の変形例＞

第３の実施の形態と異なる点を中心に説明する。ここでは、公開鍵を自由に設定可能なＩＤ暗号を用いる。なお、ここで用いるＩＤ暗号は、ＩＤ情報に基く公開鍵暗号処理である。この場合の具体例を以下に説明する。なお、ここでは、ＩＤ情報を指紋模様の特徴点からなる情報とする。また、ＩＤ情報に基く公開鍵暗号処理については、公知技術であるため、説明は省略する。なお、Ａ．Ｓｈａｍｉｒ著による「Ｉｄｅｎｔｉｔｙ－Ｂａｓｅｄ ｃｒｙｐｔｏｓｙｓｔｅｍｓ ａｎｄ ｓｉｇｎａｔｕｒｅ ｓｃｈｅｍｅｓ．」（Ｉｎ Ａｄｖａｎｃｅｓ ｉｎ Ｃｒｙｐｔｏｌｏｇｙ － ＣＲＹＰＴＯ’８４，Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ ＬＮＣＳ １９６，４７－５３，１９８４．）にて

、ＩＤ情報に基く公開鍵暗号処理についての詳細な記述がある。

【０２０６】

身元認証システム１Ｂは、さらに、認証カード１０Ｂの着脱が可能なサーバ装置を備え、サーバ装置は、カードリーダ３０Ｂの指紋読取部３１０Ｂと同様の動作を行うサーバ用指紋読取部を有している。サーバ装置は、認証カード１０Ｂが装着され、サーバ用指紋読取部より認証カード１０Ｂを所有する訪問者の指紋模様を読み取り、読み取った指紋模様を用いて、指紋模様の特徴点からなる指紋情報を生成する。次に、生成した指紋情報と秘密鍵を生成するアルゴリズムとを用いて、生成した指紋情報に対応する秘密鍵である身元証明鍵「ＳＫ」を生成し、生成した身元証明鍵「ＳＫ」を認証カード１０Ｂの証明鍵記憶部１０１Ｂへ書き込む。

【０２０７】

カードリーダ３０Ｂは、認証カード１０Ｂが挿入されたことを検知すると、要求情報を表示し、指紋読取部３１０Ｂより訪問者の指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報と検知情報とをユーザ端末２０Ｂへ出力する。

ユーザ端末２０Ｂは、カードリーダ３０Ｂより身元認証指紋情報と検知情報とを受け取り、受け取った身元認証指紋情報と公開鍵を生成するアルゴリズムとを用いて、身元認証指紋情報に対応する公開鍵「ＰＫ」を生成する。さらに、ユーザ端末２０Ｂは、乱数「Ｎ」をも生成し、生成した乱数「Ｎ」を乱数記憶領域２５０Ｂに記憶し、さらに、生成した乱数「Ｎ」を生成した公開鍵「ＰＫ」を用いて、暗号化情報Ｅｎｃ（ＰＫ、Ｎ）を生成し、生成した暗号化情報Ｅｎｃ（ＰＫ、Ｎ）をカードリーダ３０Ｂを介して認証カード１０Ｂへ出力する。以降は、上記で示した動作と同様であるため、説明は省略する。なお、認証処理の終了時は、乱数記憶領域２５０Ｂにて記憶している乱数「Ｎ」の消去を行う。

【０２０８】

これにより、バイオメトリックス情報と公開鍵暗号処理とを用いた認証方法が実現できる。

＜第４の実施の形態の変形例＞

上記で示した第３の実施の形態の変形例と同様であるため、説明は省略する。なお、カードリーダ３０Ｃに挿入された認証カードが正当な認証カードであると認証した場合には、身元認証システム１Ｃは、訪問鍵認証処理以降の動作を行う。

【０２０９】

（ｂ）認証を行う毎に異なる電子署名を用いる場合

ここでは、各実施の形態ごとに、認証を行う毎に異なる電子署名を用いた場合の変形例について説明する。

＜第１の実施の形態の変形例＞

認証を行う毎に異なる電子署名を用いた場合の身元認証システムについて、第１の実施の形態と異なる点を中心に説明する。ここで、電子署名は、一例として、有限体上のエルガマル署名である。有限体上のエルガマル署名は公知であるので説明は省略する。

【０２１０】

認証カード１０は、身元証明鍵「ＳＫ１」を秘密鍵として、証明鍵ＩＤと対応付けて記憶している。

ユーザ端末２０は、認証鍵記憶部２０１にて、公開鍵である身元認証鍵と、身元認証鍵を識別する認証鍵ＩＤとからなる組を複数記憶している。なお、以降では、身元証明鍵「ＳＫ１」に対応する公開鍵である身元認証鍵を「ＰＫ１」として説明を行う。

【０２１１】

ユーザ端末２０は、カードリーダ３０より検知情報と証明鍵ＩＤとを受け取ると、受け取った証明鍵ＩＤをＩＤ記憶領域２５１に記憶する。次に、ユーザ端末２０は、乱数「Ｎ」を生成し、生成した乱数「Ｎ」を乱数記憶領域２５０に記憶し、さらに、生成した乱数「Ｎ」をカードリーダ３０を介して認証カード１０へ出力する。

認証カード１０は、ユーザ端末２０より乱数「Ｎ」を受け取ると、記憶している身元証

明鍵「ＳＫ１」を用いて、受け取った乱数「Ｎ」の電子署名を生成し、生成した電子署名をカードリーダ３０を介してユーザ端末２０へ出力する。

【０２１２】

ユーザ端末２０は、認証カード１０より電子署名を受け取ると、ＩＤ記憶領域２５１にて記憶している証明鍵ＩＤと一致する認証鍵ＩＤに対応付けられた身元認証鍵「ＰＫ１」を認証鍵記憶部２０１より取得し、取得した身元認証鍵「ＰＫ１」と、乱数「Ｎ」とを用いて、受け取った電子署名の署名検証を行う。ここで、署名検証は、電子署名が正当なものであるか否かを検証するアルゴリズムである。正当な電子署名であると判断する場合には、カードリーダ３０に挿入された認証カードが正当な認証カードであると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。不正な電子署名であると判断する場合には、カードリーダ３０に挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。次に、ユーザ端末２０は、乱数記憶領域２５０にて記憶している乱数「Ｎ」、及びＩＤ記憶領域２５１にて記憶している証明鍵ＩＤをそれぞれ消去する。

【０２１３】

＜第２の実施の形態の変形例＞

第２の実施の形態と異なる点を中心に説明する。認証カード１０Ａは、秘密鍵である、訪問者に対応する身元証明鍵「ＳＫ１」を認証鍵記憶部２０１Ａにて記憶している。また、ユーザ端末２０Ａは、事前に配信装置５０Ａより配信された公開鍵である身元認証鍵「ＰＫ１」を記憶している。認証時の動作について、以下に説明する。ユーザ端末２０Ａは、カードリーダ３０Ａより検知情報を受け取ると、乱数「Ｎ」を生成し、生成した乱数「Ｎ」を乱数記憶領域２５０Ａに記憶し、さらに、生成した乱数「Ｎ」をカードリーダ３０Ａを介して認証カード１０Ａへ出力する。

【０２１４】

次に、上記で示した動作と同様に、認証カード１０Ａでは、乱数「Ｎ」の電子署名を生成して、生成した電子署名をユーザ端末２０Ａへ出力し、ユーザ端末２０Ａでは、事前に配信されている身元認証鍵と乱数「Ｎ」とを用いて、受け取った電子署名の署名検証を行う。以降は、上記と同様であるため、説明は省略する。なお、認証処理の終了時は、乱数記憶領域２５０Ａにて記憶している乱数「Ｎ」の消去及び認証鍵記憶部２０１Ａにて記憶している身元認証鍵「ＰＫ１」の消去を行う。

【０２１５】

＜第３の実施の形態の変形例＞

第３の実施の形態と異なる点を中心に説明する。ここでは、公開鍵を自由に設定可能なＩＤ署名を用いる。なお、ここで用いるＩＤ署名は、ＩＤ情報に基く電子署名方式であり、ＩＤ情報は指紋模様の特徴点からなる情報とする。ＩＤ署名については、公知技術であるため、説明は省略する。なお、Ａ．Ｓｈａｍｉｒ著による「Ｉｄｅｎｔｉｔｙ－Ｂａｓｅｄ ｃｒｙｐｔｏｓｙｓｔｅｍｓ ａｎｄ ｓｉｇｎａｔｕｒｅ ｓｃｈｅｍｅｓ．」（Ｉｎ Ａｄｖａｎｃｅｓ ｉｎ Ｃｒｙｐｔｏｌｏｇｙ － ＣＲＹＰＴＯ’８４，Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ ＬＮＣＳ １９６，４７－５３，１９８４．）にて、ＩＤ署名についての詳細な記述がある。

【０２１６】

ＩＤ署名を用いた場合の具体例を以下に説明する。

身元認証システム１Ｂは、さらに、認証カード１０Ｂの着脱が可能なサーバ装置を備え、サーバ装置は、カードリーダ３０Ｂの指紋読取部３１０Ｂと同様の動作を行うサーバ用指紋読取部を有している。サーバ装置は、認証カード１０Ｂが装着され、サーバ用指紋読取部より認証カード１０Ｂを所有する訪問者の指紋模様を読み取り、読み取った指紋模様を用いて、指紋模様の特徴点からなる指紋情報を生成する。次に、生成した指紋情報と秘密鍵を生成するアルゴリズムとを用いて、生成した指紋情報に対応する秘密鍵である身元証明鍵「ＳＫ」を生成し、生成した身元証明鍵「ＳＫ」を認証カード１０Ｂの証明鍵記憶部１０１Ｂへ書き込む。

【０２１７】
カードリーダ３０Ｂは、認証カード１０Ｂが挿入されたことを検知すると、要求情報を表示し、指紋読取部３１０Ｂより訪問者の指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報と検知情報とをユーザ端末２０Ｂへ出力する。
ユーザ端末２０Ｂは、カードリーダ３０Ｂより身元認証指紋情報と検知情報を受け取ると、受け取った身元認証指紋情報を認証鍵記憶部２０１Ｂへ書き込む。次に、ユーザ端末２０Ｂは、乱数「Ｎ」を生成し、生成した乱数「Ｎ」をカードリーダ３０Ｂを介して認証カード１０Ｂへ出力し、生成した乱数「Ｎ」を乱数記憶領域２５０Ｂに記憶する。
【０２１８】
認証カード１０Ｂは、ユーザ端末２０Ｂより乱数「Ｎ」を受け取ると、記憶している身元証明鍵「ＳＫ」を用いて、受け取った乱数「Ｎ」の電子署名を生成し、生成した電子署名をカードリーダ３０Ｂを介してユーザ端末２０Ｂへ出力する。
ユーザ端末２０Ｂは、認証カード１０Ｂより電子署名を受け取ると、認証鍵記憶部２０１Ｂにて記憶している身元認証指紋情報を取得し、取得した身元認証指紋情報と公開鍵を生成するアルゴリズムとを用いて、身元認証指紋情報に対応する公開鍵「ＰＫ」を生成する。生成した身元認証鍵「ＰＫ」と、乱数「Ｎ」とを用いて、受け取った電子署名の署名検証を行う。
【０２１９】
以降は、上記と同様の動作であるため、説明は省略する。
＜第４の実施の形態の変形例＞
上記で示した第３の実施の形態の変形例と同様であるため、説明は省略する。なお、カードリーダ３０Ｃに挿入された認証カードが正当な認証カードであると認証した場合には、身元認証システム１Ｃは、訪問鍵認証処理以降の動作を行う。
【０２２０】
（ｃ）固定の電子署名を用いる場合
ここでは、各実施の形態ごとに、固定の電子署名を用いた場合の変形例について説明する。
＜第１の実施の形態の変形例＞
固定の電子署名を用いた場合の身元認証システムについて、第１の実施の形態と異なる点を中心に説明する。ここで、電子署名は、一例として、有限体上のエルガマル署名である。有限体上のエルガマル署名は公知であるので説明は省略する。
【０２２１】
身元認証システム１は、さらに、認証カード１０の着脱が可能なサーバ装置を備え、サーバ装置は、身元証明鍵として電子署名を生成する秘密鍵「ＳＫ」を証明鍵ＩＤと対応付けて記憶している。認証カード１０は、証明鍵ＩＤと身元証明鍵とを記憶する代わりに、認証カード１０を識別するため識別子「ＩＤ」を記憶している。
また、ユーザ端末２０は、認証鍵ＩＤと身元認証鍵とを記憶する代わりに、身元認証鍵として公開鍵「ＰＫ」を認証鍵ＩＤと対応付けて認証鍵記憶部２０１にて記憶している。
【０２２２】
サーバ装置は、認証カード１０が装着されると、認証カード１０に記憶されている識別子「ＩＤ」を取得し、記憶している秘密鍵「ＳＫ」を用いて、取得した識別子「ＩＤ」の電子署名を生成し、生成した電子署名と秘密鍵「ＳＫ」と対応する証明鍵ＩＤとを認証カード１０に書き込む。
カードリーダ３０は、認証カード１０が挿入されたことを検知すると、認証カード１０にて記憶している電子署名と証明鍵ＩＤと識別子「ＩＤ」とを読み出し、読み出した電子署名と証明鍵ＩＤと識別子「ＩＤ」とをユーザ端末２０へ出力する。
【０２２３】
ユーザ端末２０は、電子署名と証明鍵ＩＤと識別子「ＩＤ」とを受け取ると、受け取った証明鍵ＩＤと一致する認証鍵ＩＤに対応する公開鍵「ＰＫ」を認証鍵記憶部２０１より

取得し、取得した公開鍵「ＰＫ」と、受け取った識別子「ＩＤ」とを用いて、受け取った電子署名の署名検証を行う。ここで、署名検証は、電子署名が正当なものであるか否かを検証するアルゴリズムである。正当な電子署名であると判断する場合には、カードリーダ３０に挿入された認証カードが正当な認証カードであると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。不正な電子署名であると判断する場合には、カードリーダ３０に挿入された認証カードが正当な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。

【０２２４】

＜第２の実施の形態の変形例＞

第２の実施の形態と異なる点を中心に説明する。身元認証システム１Ａは、さらに、上記と同様の動作を行うサーバ装置を備える。配信装置５０Ａは、身元認証鍵を記憶及びユーザ端末２０Ａへ配信する代わりに、公開鍵「ＰＫ」を記憶、及びユーザ端末２０Ａへ配信する。認証カード１０Ａは、身元証明鍵を記憶する代わりに、認証カード１０Ａを識別するため識別子「ＩＤ」を記憶している。また、ユーザ端末２０Ａは、事前に配信装置５０Ａより配信された身元認証鍵を記憶する代わりに、事前に配信装置５０Ａより配信された公開鍵「ＰＫ」を記憶している。

【０２２５】

なお、認証時の動作については、上記と同様の動作であるため、説明は省略する。また、配信装置５０Ａとサーバ装置とは、同一の装置であってもよい。

＜第３の実施の形態の変形例＞

第３の実施の形態と異なる点を中心に説明する。ここでは、公開鍵を自由に設定可能なＩＤ署名を用いる。なお、ここで用いるＩＤ署名は、ＩＤ情報に基く電子署名であり、ＩＤ情報は、指紋模様の特徴点からなる情報とする。この場合の具体例を以下に説明する。

【０２２６】

身元認証システム１Ｂは、さらに、認証カード１０Ｂの着脱が可能なサーバ装置を備え、サーバ装置は、カードリーダ３０Ｂの指紋読取部３１０Ｂと同様の動作を行うサーバ用指紋読取部を有している。認証カード１０Ｂは、証明鍵ＩＤと身元証明鍵とを記憶する代わりに、認証カード１０Ｂを識別するため識別子「ＩＤ」を記憶している。

サーバ装置は、認証カード１０Ｂが装着され、サーバ用指紋読取部より認証カード１０Ｂを所有する訪問者の指紋模様を読み取り、読み取った指紋模様を用いて、指紋模様の特徴点からなる指紋情報を生成する。次に、生成した指紋情報と秘密鍵を生成するアルゴリズムとを用いて、生成した指紋情報に対応する秘密鍵「ＳＫ」を生成する。さらに、サーバ装置は、挿入された認証カード１０Ｂに記憶されている識別子「ＩＤ」を取得し、生成した秘密鍵「ＳＫ」を用いて、取得した識別子「ＩＤ」の電子署名を生成し、生成した電子署名を認証カード１０Ｂに書き込む。

【０２２７】

カードリーダ３０Ｂは、認証カード１０Ｂが挿入されたことを検知すると、要求情報を表示し、指紋読取部３１０Ｂより訪問者の指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成する。さらに、認証カード１０Ｂにて記憶している電子署名と識別子「ＩＤ」とを読み出し、読み出した電子署名と識別子「ＩＤ」と生成した身元認証指紋情報とをユーザ端末２０Ｂへ出力する。

【０２２８】

ユーザ端末２０Ｂは、カードリーダ３０Ｂより電子署名と識別子「ＩＤ」と身元認証指紋情報とを受け取ると、受け取った身元認証指紋情報と公開鍵を生成するアルゴリズムとを用いて、身元認証指紋情報に対応する公開鍵「ＰＫ」を生成する。ユーザ端末２０Ｂは、生成した公開鍵「ＰＫ」と、受け取った識別子「ＩＤ」とを用いて、受け取った電子署名の署名検証を行う。以降は、上記で示した動作と同様であるため、説明は省略する。

【０２２９】

＜第４の実施の形態の変形例＞

上記で示した第３の実施の形態の変形例と同様であるため、説明は省略する。なお、カ

ードリーダ３０Ｃに挿入された認証カードが正当な認証カードであると認証した場合には、身元認証システム１Ｃは、訪問鍵認証処理以降の動作を行う。

（２）上記第１、第２、第３及び第４の実施の形態において、認証方法をチャレンジレスポンス方式としたが、これに限定されない。他の認証方法を用いてもよい。

【０２３０】

例えば、一方向性の認証である。この場合の認証方法について、第１の実施の形態に基いて、以下に説明する。

認証カード１０は、カードリーダ３０に挿入されると、乱数「Ｎ」を生成し、生成した乱数「Ｎ」に記憶している身元証明鍵「ＳＫ１」を用いて暗号化し、暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を生成する。次に、認証カード１０は、生成した乱数「Ｎ」と暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）とをカードリーダ３０を介してユーザ端末２０へ出力する。

【０２３１】

ユーザ端末２０は、認証カード１０より乱数「Ｎ」と暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）とを受け取ると、受け取った暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を記憶している身元認証鍵「ＳＫ１」を用いて、復号する。ユーザ端末２０は、復号して得られた復号結果と認証カード１０より受け取った乱数「Ｎ」とが一致するか否かを判断し、一致すると判断する場合には、カードリーダ３０に挿入された認証カードが正当な認証カードであると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。一致しないと判断する場合には、カードリーダ３０に挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。

【０２３２】

また、第２の実施の形態においては、認証カード１０Ａは、上記にて示した動作と同様の動作を行う。ユーザ端末２０Ａは、認証カード１０Ａより受け取った乱数「Ｎ」と暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）と、配信装置５０Ａより事前に受け取り、記憶している身元認証鍵とを用いて、上記にて示した動作と同様の動作を行う。なお、認証後は、事前に記憶している身元認証鍵を消去する。

【０２３３】

また、第３の実施の形態においては、認証カード１０Ｂは、上記にて示した動作と同様の動作を行う。ユーザ端末２０Ｂは、認証カード１０Ｂより受け取った乱数「Ｎ」と暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）と、カードリーダ３０Ｂより受け取った身元認証指紋情報とを用いて、上記にて示した動作と同様の動作を行う。

また、第４の実施の形態においては、認証カード１０Ｃは、上記にて示した動作と同様の動作を行う。ユーザ端末２０Ｃは、認証カード１０Ｃより受け取った乱数「Ｎ」と暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）と、カードリーダ３０Ｃより受け取った身元認証指紋情報とを用いて、上記にて示した動作と同様の動作を行う。

【０２３４】

（３）上記第１、第２、第３及び第４の実施の形態において、認証カードをカードリーダへ挿入して、認証を行ったが、これに限定されない。

カードリーダの表面にセンサー部を設け、認証カードをセンサー部へ接触させることにより認証を行ってもよい。

または、認証カードに無線タグを備え付け、センサー部とは非接触とすることによる認証を行ってもよい。

【０２３５】

（４）上記第１、第２、第３及び第４の実施の形態において、ユーザ端末とカードリーダとをケーブルにて接続したが、これに限定されない。

ユーザ端末とカードリーダとを無線による通信にて接続してもよい。

（５）上記第１、第２、第３及び第４の実施の形態において、認証結果をユーザ端末に表示したが、これに限定されない。

【０２３６】

認証により、正当な訪問者であると判断する場合には、玄関のドアの鍵を解除するよう

にしてもよい。この場合、玄関のドアは電子ロックにて鍵の施錠及び解除を行う。鍵の施錠及び解除を行う構成部を玄関制御部と呼ぶ。ユーザ端末は、カードリーダに挿入された認証カードが正当な認証カードであると認証した場合には、正当訪問者情報を生成し、生成した正当訪問者情報を玄関制御部に出力し、カードリーダに挿入された認証カードが不正な認証カードであると認証した場合には、不正訪問者情報を生成し、生成した不正訪問者情報を玄関制御部へ出力する。玄関制御部は、ユーザ端末より受け取った情報が正当訪問者情報及び不正訪問者情報のうち何れかであるかを判断し、正当訪問者情報であると判断する場合には、鍵の解除を行い、不正訪問者情報であると判断する場合には、鍵の解除を行わない。

【０２３７】

（６）ユーザ端末と認証カードとの通信方法は、上記第１、第２、第３及び第４の実施の形態にて示した通信方法に限定されない。他の通信方法を用いてもよい。

例えば、図３０にて示す身元認証システム１Ｄの構成であってもよい。

身元認証システム１Ｄについて、一例として、第１の実施の形態と異なる点を中心に以下に説明する。

【０２３８】

（Ａ）　身元認証システム１Ｄの概要

身元認証システム１Ｄは、認証カード１０Ｄ、１１Ｄ、・・・、１２Ｄ、ユーザ端末２０Ｄ、第１入出力装置６０Ｄ及び認証カードの着脱可能な第２入出力装置７０Ｄとから構成される。ここでは、身元認証システム１Ｄの概要について説明を認証カード１０Ｄとユーザ端末２０Ｄと第１入出力装置６０Ｄと第２入出力装置７０Ｄとを用いて行う。

【０２３９】

ユーザ端末２０Ｄは、利用者の宅内に配置されており、第１入出力装置６０Ｄは、利用者の宅外（例えば、玄関先）に配置されており、ユーザ端末２０Ｄと第１入出力装置６０Ｄとは、ケーブル４０Ｄにて接続されている。

身元認証システム１Ｄは、認証カード１０Ｄが第２入出力装置７０Ｄに装着されると、第１入出力装置６０Ｄと第２入出力装置７０Ｄとの間にて情報の入出力を行うことにより、第１の実施の形態にて示した認証処理を行う。ここでは、第１入出力装置６０Ｄと第２入出力装置７０Ｄとの間における情報の入出力をＱＲコードからなる画像情報を用いて行う。画像情報のやりとりは、以下のようにして行う。ユーザ端末２０Ｄが画像情報を受け取る場合には、第１入出力装置６０Ｄの画像受取部６０１Ｄを用いて、第２入出力装置７０Ｄの表示部７０３Ｄにて表示された画像情報を受け取る。また、認証カード１０Ｄが画像情報を受け取る場合には、第２入出力装置７０Ｄの画像受取部７０２Ｄを用いて、第１入出力装置６０Ｄの表示部６０２Ｄにて表示された画像情報を受け取る。

【０２４０】

なお、身元認証システム１Ｄにおいて、認証カード１１Ｄ、・・・、１２Ｄが第２入出力装置７０Ｄに装着された場合も同様の動作を行うため、説明は省略する。

（Ｂ）　認証カード１０Ｄの構成

ここでは、認証カード１０Ｄの構成について説明する。認証カード１０Ｄは、ＩＣを内蔵している可搬型の記録媒体であり、一例として、ＩＣカード機能付メモリカードである。認証カード１０Ｄは、図３１に示すように、証明鍵記憶部１０１Ｄ、制御部１０２Ｄ及び入出力部１０３Ｄから構成されている。

【０２４１】

認証カード１０Ｄは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＲＯＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード１０Ｄは、その機能を達成する。

なお、認証カード１１Ｄ、・・・、１２Ｄは、認証カード１０Ｄと同様の構成を有しているため、説明は省略する。

【０２４２】

（ａ）　証明鍵記憶部１０１Ｄ、入出力部１０３Ｄ
証明鍵記憶部１０１Ｄ及び入出力部１０３Ｄは、それぞれ証明鍵記憶部１０１及び入出力部１０３と同様であるため、説明は省略する。
（ｂ）　制御部１０２Ｄ
制御部１０２Ｄは、第２入出力装置７０Ｄより入出力部１０３Ｄを介して、証明鍵ＩＤを要求する旨のＩＤ要求情報を受け取ると、証明鍵記憶部１０１Ｄより証明鍵ＩＤを取得する。制御部１０２Ｄは、取得した証明鍵ＩＤを用いて、ＩＤ用ＱＲコードを生成し、生成したＩＤ用ＱＲコードを入出力部１０３Ｄを介して第２入出力装置７０Ｄへ出力する。
【０２４３】
さらに、制御部１０２Ｄは、第２入出力装置７０Ｄより乱数「Ｎ」を示す乱数用ＱＲコードを受け取ると、受け取った乱数用ＱＲコードより乱数「Ｎ」を生成する。次に、制御部１０２Ｄは、証明鍵記憶部１０１Ｄより身元証明鍵「ＳＫ１」を取得し、取得した身元証明鍵「ＳＫ１」を用いて、乱数用ＲＱコードより生成した乱数「Ｎ」に対して暗号化を施し、暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を生成する。制御部１０２Ｄは、生成した暗号化情報を暗号化用ＱＲコードを生成し、生成した暗号化用ＱＲコードを入出力部１０３Ｄを介して第２入出力装置７０Ｄへ出力する。
【０２４４】
（Ｃ）　第２入出力装置７０Ｄ
ここでは、第２入出力装置７０Ｄの構成について説明する。第２入出力装置７０Ｄは、図３１に示すように、カード読取部７０１Ｄ、画像受取部７０２Ｄ及び表示部７０３Ｄから構成されている。
第２入出力装置７０Ｄは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＲＯＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、第２入出力装置７０Ｄは、その機能を達成する。
【０２４５】
（ａ）　カード読取部７０１Ｄ
カード読取部７０１Ｄは、認証カード１０Ｄが装着されたことの検知を行う。カード読取部７０１Ｄは、認証カード１０Ｄが挿入されたことを検知すると、ＩＤ要求情報を生成し、生成したＩＤ要求情報を認証カード１０Ｄへ出力する。次に、認証カード１０ＤよりＩＤ用ＱＲコードを受け取ると、受け取ったＩＤ用ＱＲコードを表示部７０３Ｄへ出力する。
【０２４６】
さらに、カード読取部７０１Ｄは、第１入出力装置６０Ｄより画像受取部７０２Ｄを介して、乱数用ＱＲコードを受け取ると、受け取った乱数用ＱＲコードを認証カード１０Ｄへ出力する。カード読取部７０１Ｄは、認証カード１０Ｄより暗号化用ＱＲコードを受け取ると、受け取った暗号化用ＱＲコードを表示部７０３Ｄへ出力する。
（ｂ）　画像受取部７０２Ｄ
画像受取部７０２Ｄは、例えばカメラであり、第１入出力装置６０Ｄにて表示されている画像を撮像し、撮像した画像をカード読取部７０１Ｄへ出力する。
【０２４７】
（ｃ）　表示部７０３Ｄ
表示部７０３Ｄは、例えばディスプレイであり、カード読取部７０１Ｄより受け取った情報を表示する。
（Ｄ）　ユーザ端末２０Ｄの構成
ここでは、ユーザ端末２０Ｄの構成について説明する。ユーザ端末２０Ｄは、認証カード１０Ｄの認証を行う。ユーザ端末２０Ｄは、図３２に示すように、認証鍵記憶部２０１Ｄ、認証部２０２Ｄ、表示部２０３Ｄ及び入出力部２０４Ｄから構成されている。
【０２４８】
ユーザ端末２０Ｄは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディ

スクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記ＲＯＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末２０Ｄは、その機能を達成する。

【０２４９】

（ａ）　認証鍵記憶部２０１Ｄ、表示部２０３Ｄ

認証鍵記憶部２０１Ｄ及び表示部２０３Ｄは、それぞれ認証鍵記憶部２０１及び表示部２０３と同様であるため、説明は省略する。

（ｂ）　認証部２０２Ｄ

認証部２０２Ｄは、乱数を記憶する乱数記憶領域２５０Ｄ及び証明鍵ＩＤを記憶するＩＤ記憶領域２５１Ｄを有している。

【０２５０】

認証部２０２Ｄは、第１入出力装置６０Ｄより入出力部２０４Ｄを介して、ＩＤ用ＱＲコードを受け取ると、受け取ったＩＤ用ＱＲコードより証明鍵ＩＤを生成し、生成した証明鍵ＩＤをＩＤ記憶領域２５１Ｄに記憶する。次に、認証部２０２Ｄは、乱数「Ｎ」を生成し、生成した乱数「Ｎ」を乱数記憶領域２５０Ｄに記憶する。また、生成した乱数「Ｎ」を用いて、乱数用ＱＲコードを生成し、生成した乱数用ＱＲコードを入出力部２０４Ｄを介して第１入出力装置６０Ｄへ出力する。さらに、認証部２０２Ｄは、第１入出力装置６０Ｄより入出力部２０４Ｄを介して、暗号化用ＱＲコードを受け取ると、受け取った暗号化用ＱＲコードを用いて暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）を生成する。次に、ＩＤ記憶領域２５１Ｄにて記憶している証明鍵ＩＤと一致する認証鍵ＩＤと対応する身元認証鍵を認証鍵記憶部２０１Ｄより取得し、取得した身元認証鍵を用いて、暗号化情報Ｅｎｃ（ＳＫ１、Ｎ）の復号を行い、復号により得られた復号結果と、乱数記憶領域２５０Ｄにて記憶している乱数「Ｎ」とが一致するか否かを判断する。一致すると判断する場合には、認証部２０２Ｄは、第２入出力装置７０Ｄに装着されている認証カードが正当な認証カードであると認証し、正当訪問者情報を生成して、生成した正当訪問者情報を表示部２０３Ｄへ出力する。。一致しないと判断する場合には、認証部２０２Ｄは、第２入出力装置７０Ｄに装着されている認証カードが不正な認証カードであると認証し、不正訪問者情報を生成して、生成した不正訪問者情報を表示部２０３Ｄへ出力する。

【０２５１】

さらに、認証部２０２Ｄは、乱数記憶領域２５０Ｄに記憶している乱数「Ｎ」の消去、及びＩＤ記憶領域２５１Ｄに記憶している証明鍵ＩＤの消去を行う。

（ｃ）　入出力部２０４Ｄ

入出力部２０４Ｄは、第１入出力装置６０Ｄより受け取った情報を認証部２０２Ｄへ出力し、認証部２０２Ｄから受け取った情報を第１入出力装置６０Ｄへ出力する。

【０２５２】

（Ｅ）　第１入出力装置６０Ｄ

ここでは、第１入出力装置６０Ｄの構成について説明する。第１入出力装置６０Ｄは、図３２に示すように、画像受取部６０１Ｄ、表示部６０２Ｄ及び入出力部６０３Ｄから構成されている。

第１入出力装置６０Ｄは、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどから構成されるコンピュータシステムである。前記ＲＯＭには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、第１入出力装置６０Ｄは、その機能を達成する。

【０２５３】

（ａ）　画像受取部６０１Ｄ

画像受取部６０１Ｄは、例えばカメラであり、第２入出力装置７０Ｄにて表示されている画像を撮像し、撮像した画像を入出力部６０３Ｄを介してユーザ端末２０Ｄへ出力する。

（ｂ）　表示部６０２Ｄ

表示部６０２Ｄは、例えばディスプレイであり、入出力部６０３Ｄを介してユーザ端末２０Ｄより受け取った情報を表示する。

【０２５４】

（Ｆ）　身元認証処理の動作

身元認証処理の動作は、第１の実施の形態にて示した身元認証処理の動作との変更点のみを説明する。先ず、カードリーダ３０にて行っていた動作を第１入出力装置６０Ｄ及び第２入出力装置７０Ｄにて行うことになる。第１入出力装置６０Ｄと第２入出力装置７０Ｄとの情報の受け渡しは、それぞれに備えられた画像受取部を用いて、相手側装置に表示されている情報を撮像する。

【０２５５】

また、ユーザ端末２０Ｄでは、認証カード１０Ｄへ出力する情報をＱＲコード化して出力するように変更し、認証カード１０Ｄより受け取る情報は、ＱＲコード化されているためＱＲコードより元の情報を生成して取得するように変更する。

認証カード１０Ｄにおいてもユーザ端末２０Ｄと同様に、ユーザ端末２０Ｄへ出力する情報をＱＲコード化して出力するように変更し、ユーザ端末２０Ｄより受け取る情報は、ＱＲコード化されているためＱＲコードより元の情報を生成して取得するように変更する。

【０２５６】

（Ｇ）　認証処理の動作

認証処理の動作は、第１の実施の形態にて示した認証処理の動作との変更点のみを説明する。ステップＳ１００を、認証カード１０Ｄより暗号化用ＱＲコードを受け取り、受け取った暗号化用ＱＲコードから暗号化情報を生成し、取得するように変更する。

（Ｈ）他の実施例への適用

これまで、第１の実施の形態と異なる点を中心に身元認証システム１Ｄの説明を行ったが、身元認証システム１Ｄにて用いたＱＲコードによる情報の受け渡しは第２、第３及び第４の実施の変形例として適用できる。

【０２５７】

つまり、身元認証システムは、訪問者は利用者宅へ訪問した際に受け渡しされる情報をＱＲコード化して、ＱＲコード化した情報の受け渡しを行えばよい。

なお、第３の実施の変形例として適用する場合には、第２入出力装置に、指紋読取部３１０Ｂと同様の指紋読取部を備えることで、実現できる。また、第４の実施の変形例として適用する場合にも、同様に第２入出力装置に、指紋読取部を備えることで、実現できる。

【０２５８】

（７）上記（６）では、ＱＲコードを用いたが、他の画像情報であってもよい。例えば、バーコードである。

また、画像情報以外のものであってもよい。例えば、光信号である。

（８）上記（６）では、情報の受け渡しを、ディスプレイによる表示とカメラによる画像の撮像により行ったが、これに限定されない。

【０２５９】

例えば、第１及び第２入出力装置に赤外線機能を設けて、赤外線通信による情報の受け渡しを行ってもよい。このとき通信に用いられる信号は赤外線信号である。

または、第１及び第２入出力装置にスピーカとマイクとを設けて、受け渡しを行う情報を音声信号に変換して、変換した音声信号による通信を行ってもよい。

（９）上記（６）において、情報の受け渡しに第１及び第２入出力装置を用いたが、これに限定されない。

【０２６０】

例えば、第１入出力装置が有する機能をユーザ端末に設けて、第２入出力装置を認証カードの着脱が可能なカメラ付携帯電話機としてもよい。このとき、情報の受け渡しは、玄関ののぞき穴を利用して行われる。

（１０）上記（６）において、ユーザ端末２０Ｄから認証カード１０Ｄへ情報を出力する方法と、認証カード１０Ｄ及び第２入出力装置７０Ｄからユーザ端末２０Ｄへ情報を出力する方法を同一の方法としたが、これに限定されない。ユーザ端末２０Ｄから認証カード１０Ｄへ情報を出力する方法と、認証カード１０Ｄ及び第２入出力装置７０Ｄからユーザ端末２０Ｄへ情報を出力する方法とをそれぞれ異なる方法としてもよい。

【０２６１】

例えば、ユーザ端末２０Ｄから認証カード１０Ｄへ情報を出力する方法としてＱＲコードを用い、認証カード１０Ｄ及び第２入出力装置７０Ｄからユーザ端末２０Ｄへ情報出力する方法として、音声信号を用いる。

（１１）上記第１、第２、第３及び第４の実施の形態において、ユーザ端末から認証カードへ出力する情報、認証カード及びカードリーダからユーザ端末へ出力する情報をそれぞれ他の情報に変換して出力してもよい。

【０２６２】

例えば、ユーザ端末から認証カードへ出力する情報をＱＲコード化して、認証カードへ出力してもよい。このとき、認証カードは、ユーザ端末よりカードリーダを介してＱＲコード化された情報を受け取ると、受け取ったＱＲコード化された情報を用いて、元の情報を生成することになる。また、同様に、認証カード及びカードリーダからユーザ端末へ出力する情報をＱＲコード化して、ユーザ端末へ出力してもよい。このとき、ユーザ端末は、認証カードよりカードリーダを介してＱＲコード化された情報やカードリーダよりＱＲコード化された情報を受け取ると、受け取ったＱＲコード化された情報を用いて、元の情報を生成することになる。

【０２６３】

なお、上記に例では、ユーザ端末から情報を出力する方法と、認証カード及びカードリーダから情報を出力する方法とを同一の方法（ＱＲコード化した情報を出力する方法）としたが、ユーザ端末から情報を出力する方法と、認証カード及びカードリーダから情報を出力する方法とをそれぞれ異なる方法としてもよい。

例えば、ユーザ端末から情報を出力する方法としてＱＲコードを用いて、認証カード及びカードリーダから情報を出力する方法として音声信号を用いる。

【０２６４】

（１２）上記第１、第２、第３及び第４の実施の形態において、認証カードに制御部を設けたが、これに限定されない。認証カードに制御部を設けないで、カードリーダに制御部を設けて、認証カード内で行っていた処理をカードリーダにて行ってもよい。

また、上記（６）においても同様に、認証カードに制御部を設けないで、第２入出力装置に制御部を設けて、認証カード内で行っていた処理を第２入出力装置にて行ってもよい。

【０２６５】

（１３）上記第１、第２、第３及び第４の実施の形態及び上記（６）において、ユーザ端末を携帯電話機としてもよい。このとき、携帯電話機は、認証部を予め備えておいてもよいし、認証部と同様の動作を行うアプリケーションを訪問業者が有するアプリケーション配信装置よりダウンロードすることにより入手して、記憶してもよい。

または、インターホンやテレビドアホンにユーザ端末の機能を備えてもよい。

【０２６６】

（１４）上記第１、第２、第３及び第４の実施の形態及び上記（６）において、認証カードがユーザ端末を識別するようにしてもよい。

このとき、ユーザ端末は、端末ＩＤを予め記憶しており、認証カードは、端末ＩＤを記憶する記憶領域を備えている。ユーザ端末は、認証後、正当な訪問者であると判断する場合に、予め記憶している端末ＩＤを認証カードへ出力する。認証カードは、受け取った端末ＩＤを記憶領域へ記憶する。

【０２６７】

これにより、記憶領域に記憶された端末ＩＤを訪問履歴として利用することができる。

（１５）上記第１、第２、第３及び第４の実施の形態及び上記（６）において、認証カードが、ユーザ端末を認証するようにしてもよい。

これにより、配達証明と同様のことが実現できる。

（１６）上記第１の実施の形態において、ユーザ端末２０に記憶している身元認証鍵の変更及びユーザ端末２０へ身元認証鍵の追加を行ってもよい。

【０２６８】

このとき、身元認証システム１は、さらに、配信装置を備え、配信装置は、ユーザ端末２０へ、認証ＩＤと身元認証鍵とからなる組を送信する。ユーザ端末２０は、配信装置より、認証ＩＤと身元認証鍵とからなる組を受信すると、受信した認証ＩＤと一致する認証ＩＤが鍵情報テーブルＴ１００に存在するか否かを判断する。存在すると判断する場合には、受信した認証ＩＤと一致する認証ＩＤに対応する身元認証鍵を受信した身元認証鍵へと書き替える。存在しないと判断する場合には、新規の身元認証鍵として、受信した認証ＩＤと身元認証鍵とからなる組を鍵情報テーブルＴ１００に追加する。

【０２６９】

（１７）上記第２の実施の形態において、身元認証鍵を配信する場合には、配信する身元認証鍵を暗号化して配信してもよい。このとき、ユーザ端末は、暗号化された身元認証鍵を復号する復号鍵を、耐タンパ性を有する記憶領域にて予め記憶しており、受信した暗号化された身元認証鍵を復号鍵にて復号を行い、復号された身元認証鍵を、耐タンパ性を有する認証鍵記憶部にて記憶する。

【０２７０】

（１８）第２の実施の形態では、配信装置５０Ａとユーザ端末２０Ａをネットワーク接続する際にインターネットを利用したが、これに限定されない。専用線によるネットワーク接続であってもよい。

（１９）第２の実施の形態において、配信装置５０Ａより事前に配信され、記憶している身元認証鍵を認証後、消去したが、これに限定されない。

【０２７１】

認証後も、消去しないで記憶しておいてもよい。このとき、ユーザ端末２０Ａは、配信装置５０Ａより身元認証鍵を受け取ると、受け取った身元認証鍵と記憶している身元認証鍵とが一致するか否かを判断し、一致すると判断する場合には、鍵の書き換えは行わず、一致しないと判断する場合には、記憶している身元認証鍵から受け取った身元認証鍵へと書き換えを行う。

【０２７２】

（２０）上記第３の実施の形態において、認証に用いるバイオメトリックス情報として指紋模様の特徴点からなる情報（以下、単に「指紋情報」という。）を用いたが、これに限定されない。

バイオメトリックス情報として、例えば、指紋情報、訪問者の声紋の特徴を示す声紋情報、訪問者の虹彩の特徴を示す虹彩情報、訪問者の顔の輪郭の特徴を示す輪郭情報、訪問者のＤＮＡの特徴を示すＤＮＡ情報又は、これら情報の組合せである。

【０２７３】

このとき、声紋情報を用いる場合は、カードリーダ３０Ｂには、訪問者の音声を受け取り、受け取った音声から訪問者の声紋の特徴を示す身元認証声紋情報を生成する声紋読取部を設け、認証カード１０Ｂには、訪問者の声紋の特徴を示す身元証明声紋情報を予め記憶しておく。

また、虹彩情報を用いる場合は、カードリーダ３０Ｂには、訪問者の虹彩を読み取り、読み取った虹彩から訪問者の虹彩の特徴を示す身元認証虹彩情報を生成する虹彩読取部を設け、認証カード１０Ｂには、訪問者の虹彩の特徴を示す身元証明虹彩情報を予め記憶しておく。

【０２７４】

また、輪郭情報を用いる場合は、カードリーダ３０Ｂには、訪問者の顔の輪郭を読み取り、読み取った顔の輪郭から訪問者の顔の輪郭の特徴を示す身元認証輪郭情報を生成する

輪郭読取部を設け、認証カード１０Ｂには、訪問者の顔の輪郭の特徴を示す身元証明輪郭情報を予め記憶しておく。

また、ＤＮＡ情報を用いる場合は、カードリーダ３０Ｂには、訪問者のＤＮＡを解析したＤＮＡ情報である身元認証ＤＮＡ情報を受け付けるＤＮＡ情報読取部を設け、認証カードには、訪問者のＤＮＡを解析したＤＮＡ情報である身元証明ＤＮＡ情報を予め記憶しておく。ここで、ＤＮＡ情報とは、例えば、訪問者の髪の毛、血液又は唾液より解析される情報である。

【０２７５】

なお、第４の実施の形態においても同様に、バイオメトリックス情報を、例えば、指紋情報、訪問者の声紋の特徴を示す声紋情報、訪問者の虹彩の特徴を示す虹彩情報、訪問者の顔の輪郭の特徴を示す輪郭情報、訪問者のＤＮＡの特徴を示すＤＮＡ情報又は、これら情報の組合せとしてもよい。

（２１）上記第３及び第４の実施の形態において、カードリーダよりユーザ端末へ出力する身元認証指紋情報を暗号化して出力してもよい。

【０２７６】

このとき、カードリーダは、身元認証指紋情報を暗号化する暗号鍵を予め記憶しており、また、ユーザ端末は、受け取った暗号化された身元認証指紋情報を復号する復号鍵を予め記憶することで実現できる。

（２２）上記第４の実施の形態にて示した訪問鍵認証処理において、チャレンジレスポンス方式による認証方法として、秘密鍵暗号処理を用いたが、これに限定されない。上記（１）と同様に、他の暗号処理を用いたチャレンジレスポンス方式による認証方法でもよいし、上記（２）と同様に他の認証方法でもよい。

【０２７７】

（２３）上記（１）の（ａ）において、公開鍵をユーザ端末、秘密鍵を認証カードへそれぞれ記憶したが、これに限定されない。

公開鍵を認証カード、秘密鍵をユーザ端末へそれぞれ記憶してもよい。このときの認証の動作は、秘密鍵暗号処理を用いた場合と同様であるため、説明は省略する。

（２４）上記第１、第２、第３及び第４の実施の形態において、身元認証システムの構成要件であるユーザ端末とカードリーダとをそれぞれ個別の装置として扱ったが、これに限定されない。

【０２７８】

ユーザ端末とカードリーダとをユーザ端末とカードリーダとからなる１つの装置して扱ってもよい。

また、上記（６）においても同様に、ユーザ端末と第１入出力装置とからなる１つの装置として扱ってもよい。

（２５）第４の実施の形態において、証明用訪問鍵と認証用訪問鍵とを基に認証を行う場合、第２乱数を生成して認証に使用したが、これに限定されない。第２乱数を生成しないで、先の認証にて使用した第１乱数を用いて、証明用訪問鍵と認証用訪問鍵とを基に認証を行ってもよい。このとき、図２６及び図２７にて示した身元認証処理においては、ステップＳ７１５を乱数記憶領域２５０Ｃにて記憶している第１乱数「Ｎ１」をカードリーダ３０Ｃへ出力するように変更し、以下の動作にて第２乱数「Ｎ２」を用いる代わりに、第１乱数「Ｎ１」を用いて動作するように変更すればよい。

【０２７９】

（２６）第４の実施の形態において、認証用訪問鍵と証明用訪問鍵とを基にした認証後に、証明用時間情報及び証明用内容情報と、認証用訪問情報に含まれる時間情報及び内容情報とがそれぞれ一致するか否かの判断、及び訪問時間帯の判断を行ったが、これに限定されない。

認証用訪問鍵と証明用訪問鍵とを基にした認証を行わないで、つまり身元認証指紋情報と身元証明情報とを基にした認証後に、証明用時間情報及び証明用内容情報と、認証用訪問情報に含まれる時間情報及び内容情報とがそれぞれ一致するか否かの判断、及び訪問時

間帯の判断を行ってもよい。

【０２８０】

または、認証用訪問鍵と証明用訪問鍵とを基にした認証を行わないで、つまり身元認証指紋情報と身元証明情報とを基にした認証後に、証明用時間情報及び証明用内容情報と、認証用訪問情報に含まれる時間情報及び内容情報とがそれぞれ一致するか否かの判断のみ行ってもよいし、訪問時間帯の判断のみ行ってもよい。

または、身元認証指紋情報と身元証明情報とを基にした認証後に、認証用訪問鍵と証明用訪問鍵とを基にした認証のみを行ってもよい。

【０２８１】

（２７）上記第１、第２及び第３の実施の形態において、認証カードの証明鍵記憶部のみが耐タンパ性を有したが、他の構成要素においても耐タンパ性を有してもよい。

例えば、上記第１の実施の形態において、認証カード１０の構成要素である証明鍵記憶部１０１、制御部１０２及び入出力部１０３の全てが耐タンパ性を有してもよい。

また、第４の実施の形態においても同様に、認証カードの証明鍵記憶部及び訪問鍵記憶部が耐タンパ性を有したが、他の構成要素においても耐タンパ性を有してもよい。

【０２８２】

（２８）上記第１、第２、第３及び第４の実施の形態において、ユーザ端末は、認証カードより受け取った暗号化情報（第４の実施の形態では、第１暗号化情報）を復号し、復号して得られた復号結果と、生成し記憶している乱数（第４の実施の形態では、第１乱数）とを用いて、復号結果と乱数（第４の実施の形態では、第１乱数）とが一致するか否かの判断を行ったが、これに限定されない。

【０２８３】

ユーザ端末は、生成し記憶している乱数（第４の実施の形態では、第１乱数）を、記憶している身元認証鍵（第３及び第４の実施の形態では、身元認証指紋情報）を用いて暗号化して、暗号化乱数を生成し、生成した暗号化乱数と、認証カードより受け取った暗号化情報とを用いて、暗号化乱数と暗号化情報とが一致するか否かの判断を行い、一致する場合には、認証カードが正当な認証であると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。一致しない場合には、認証カードが不正な認証であると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。

【０２８４】

（２９）上記第１、第２、第３及び第４の実施の形態において、ユーザ端末は、生成した乱数（第４の実施の形態では、第１乱数）を認証カードへ出力したが、身元認証鍵（第３及び第４の実施の形態では、身元認証指紋情報）を用いて、乱数を暗号化して暗号化乱数を生成し、生成した暗号化乱数を出力してもよい。

このとき、認証カードでは、ユーザ端末より受け取った暗号化乱数を、身元証明鍵を用いて復号して得られた復号結果をユーザ端末へ出力し、ユーザ端末では、認証カードより受け取った復号結果と、記憶している乱数（第４の実施の形態では、第１乱数）とが一致するか否かの判断を行う。一致する場合には、認証カードが正当な認証であると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。一致しない場合には、認証カードが不正な認証であると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。

【０２８５】

（３０）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＢＤ（Ｂｌｕ－ｒａｙ　Ｄｉｓｃ）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【０２８６】
また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。
また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。
【０２８７】
また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。
（３１）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。
【産業上の利用可能性】
【０２８８】
上記において説明した身元認証システムは、訪問業者による訪問者が利用者宅に訪問して、セールス、宅配サービス、その他サービスの提供などを行う産業において、経営的、つまり反復的かつ継続的に利用されうる。
【図面の簡単な説明】
【０２８９】
【図１】身元認証システム１の全体の概要を示す図である。
【図２】認証カード１０の構成を示すブロック図である。
【図３】ユーザ端末２０及びカードリーダ３０の構成を示すブロック図である。
【図４】認証鍵記憶部２０１が有する鍵情報テーブルＴ１００のデータ構造を示す。
【図５】身元認証システム１における身元認証処理の動作を示す流れ図である。
【図６】身元認証システム１における認証処理の動作を示す流れ図である。
【図７】身元認証システム１Ａの全体の概要を示す図である。
【図８】配信装置５０Ａの構成を示すブロック図である。
【図９】配信鍵記憶部５０１Ａが有する配信鍵情報テーブルＴ２００のデータ構造を示す。
【図１０】認証カード１０Ａの構成を示すブロック図である。
【図１１】ユーザ端末２０Ａ及びカードリーダ３０Ａの構成を示すブロック図である。
【図１２】身元認証システム１Ａにおける配信処理の動作を示す流れ図である。
【図１３】身元認証システム１Ａにおける身元認証処理の動作を示す流れ図である。
【図１４】身元認証システム１Ａにおける認証処理の動作を示す流れ図である。
【図１５】身元認証システム１Ｂの全体の概要を示す図である。
【図１６】認証カード１０Ｂの構成を示すブロック図である。
【図１７】ユーザ端末２０Ｂ及びカードリーダ３０Ｂの構成を示すブロック図である。
【図１８】身元認証システム１Ｂにおける身元認証処理の動作を示す流れ図である。
【図１９】身元認証システム１Ｂにおける認証処理の動作を示す流れ図である。
【図２０】身元認証システム１Ｃの全体の概要を示す図である。
【図２１】配信装置５０Ｃの構成を示すブロック図である。
【図２２】認証カード１０Ｃの構成を示すブロック図である。
【図２３】訪問鍵記憶部１０５Ｃが有する証明用訪問情報テーブルＴ３００のデータ構造を示す。
【図２４】ユーザ端末２０Ｃ及びカードリーダ３０Ｃの構成を示すブロック図である。
【図２５】身元認証システム１Ｃにおける訪問情報配信処理の動作を示す流れ図である。

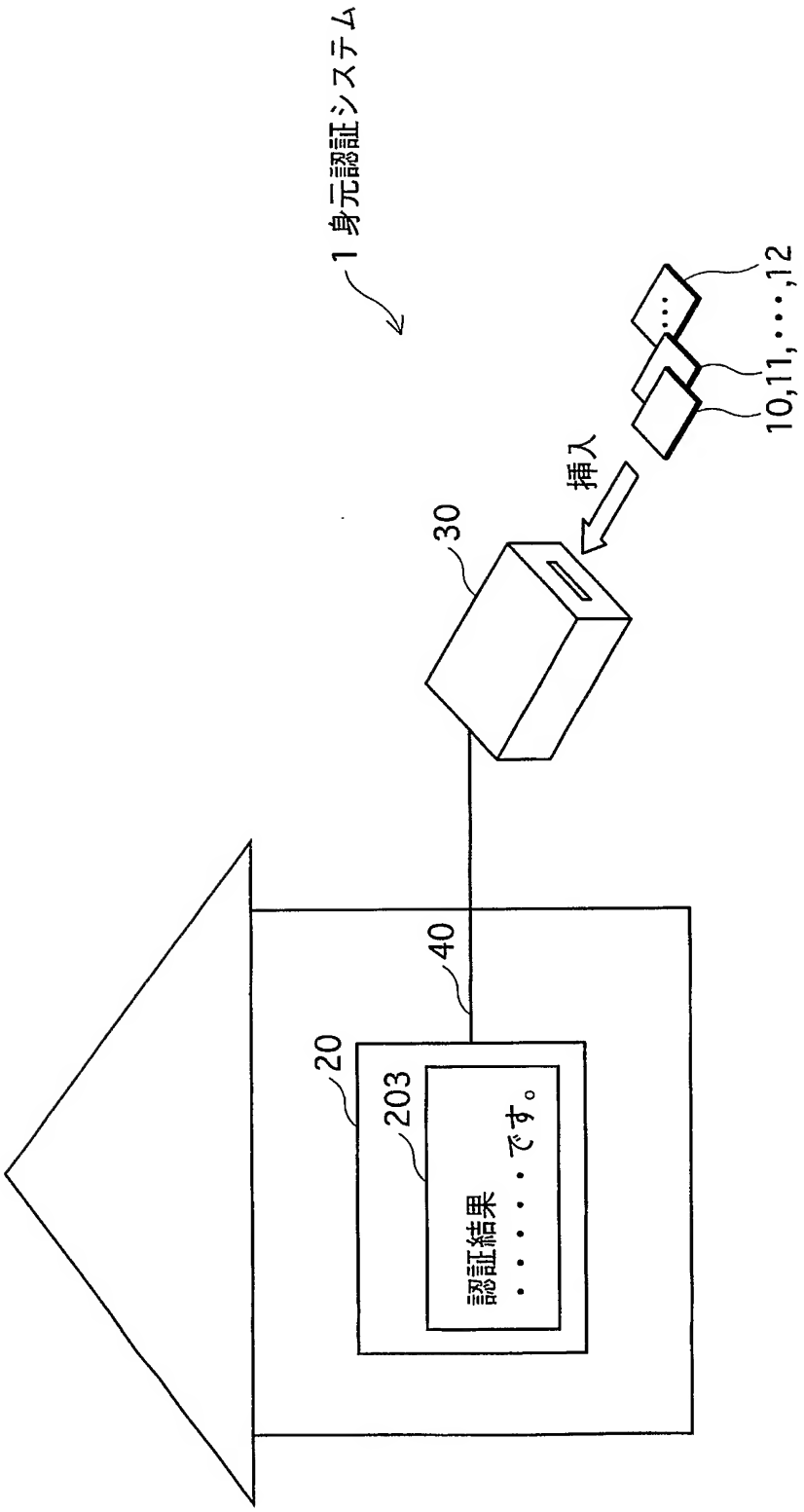
【図２６】身元認証システム１Ｃにおける身元認証処理の動作を示す流れ図である。図２７へ続く。
【図２７】身元認証システム１Ｃにおける身元認証処理の動作を示す流れ図である。図２６から続く。
【図２８】身元認証システム１Ｃにおける訪問鍵認証処理の動作を示す流れ図である。
【図２９】身元認証システム１Ｃにおける訪問情報検証処理の動作を示す流れ図である。
【図３０】身元認証システム１Ｄの全体の概要を示す図である。
【図３１】認証カード１０Ｄ及び第２入出力装置７０Ｄの構成を示すブロック図である。
【図３２】ユーザ端末２０Ｄ及び第１入出力装置６０Ｄの構成を示すブロック図である。

【符号の説明】

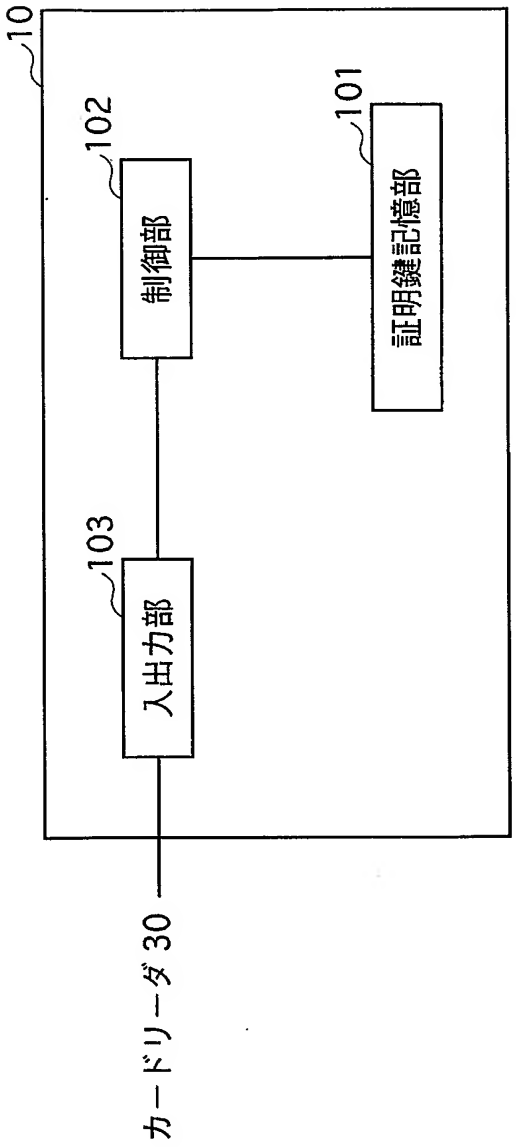
【０２９０】

１　　身元認証システム
１０～１２　　認証カード
２０　　ユーザ端末
３０　　カードリーダ
４０　　ケーブル
１０１　　証明鍵記憶部
１０２　　制御部
１０３　　入出力部
２０１　　認証鍵記憶部
２０２　　認証部
２０３　　表示部
２０４　　入出力部
２５０　　乱数記憶領域
２５１　　ＩＤ記憶領域
３０１　　カード読取部
３０２　　入出力部
３０３　　表示部

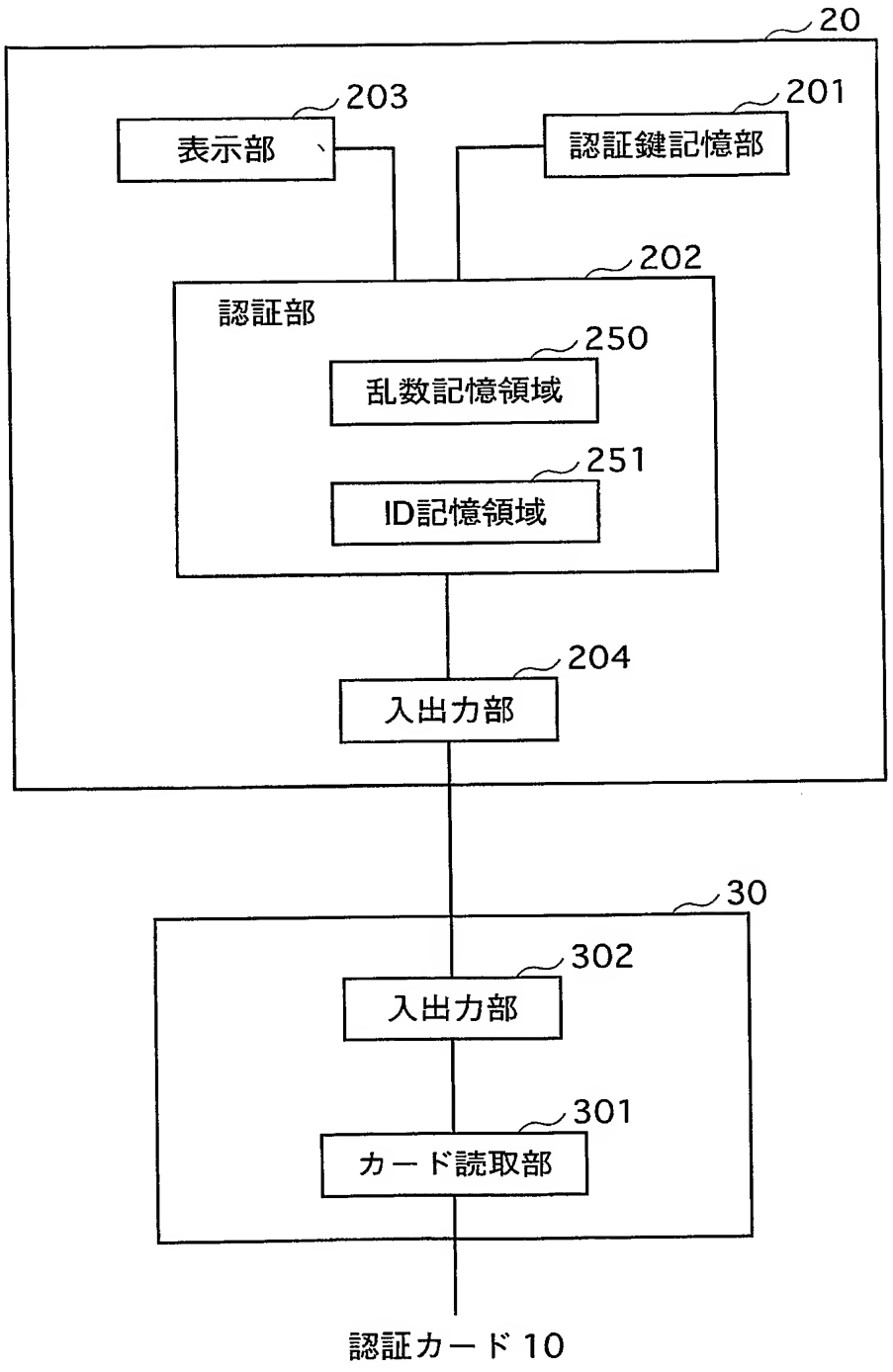
【書類名】図面
【図１】



【図２】



【図３】

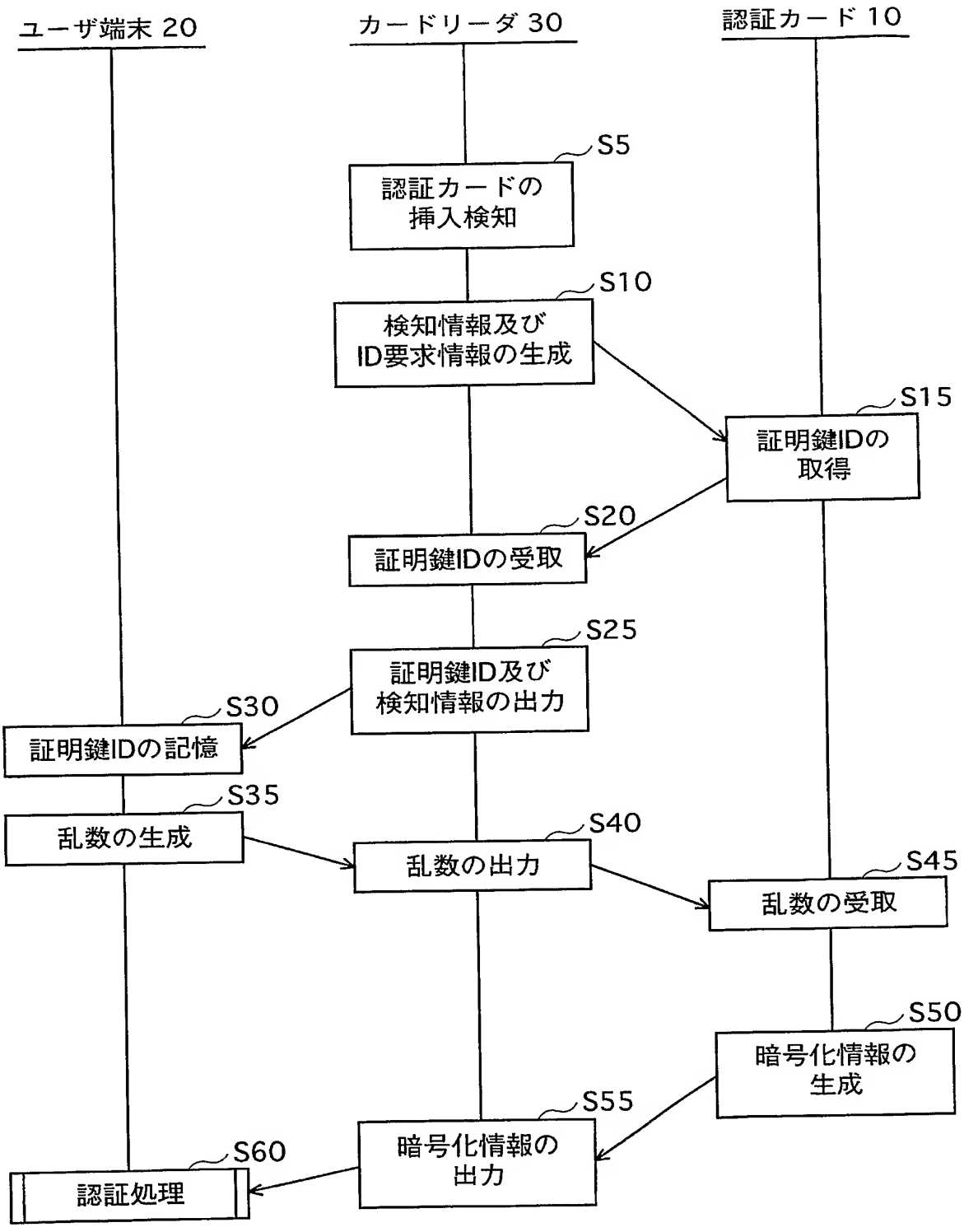

20
203
表示部
201
認証鍵記憶部
202
認証部
250
乱数記憶領域
251
ID記憶領域
204
入出力部
30
302
入出力部
301
カード読取部
認証カード10

【図４】

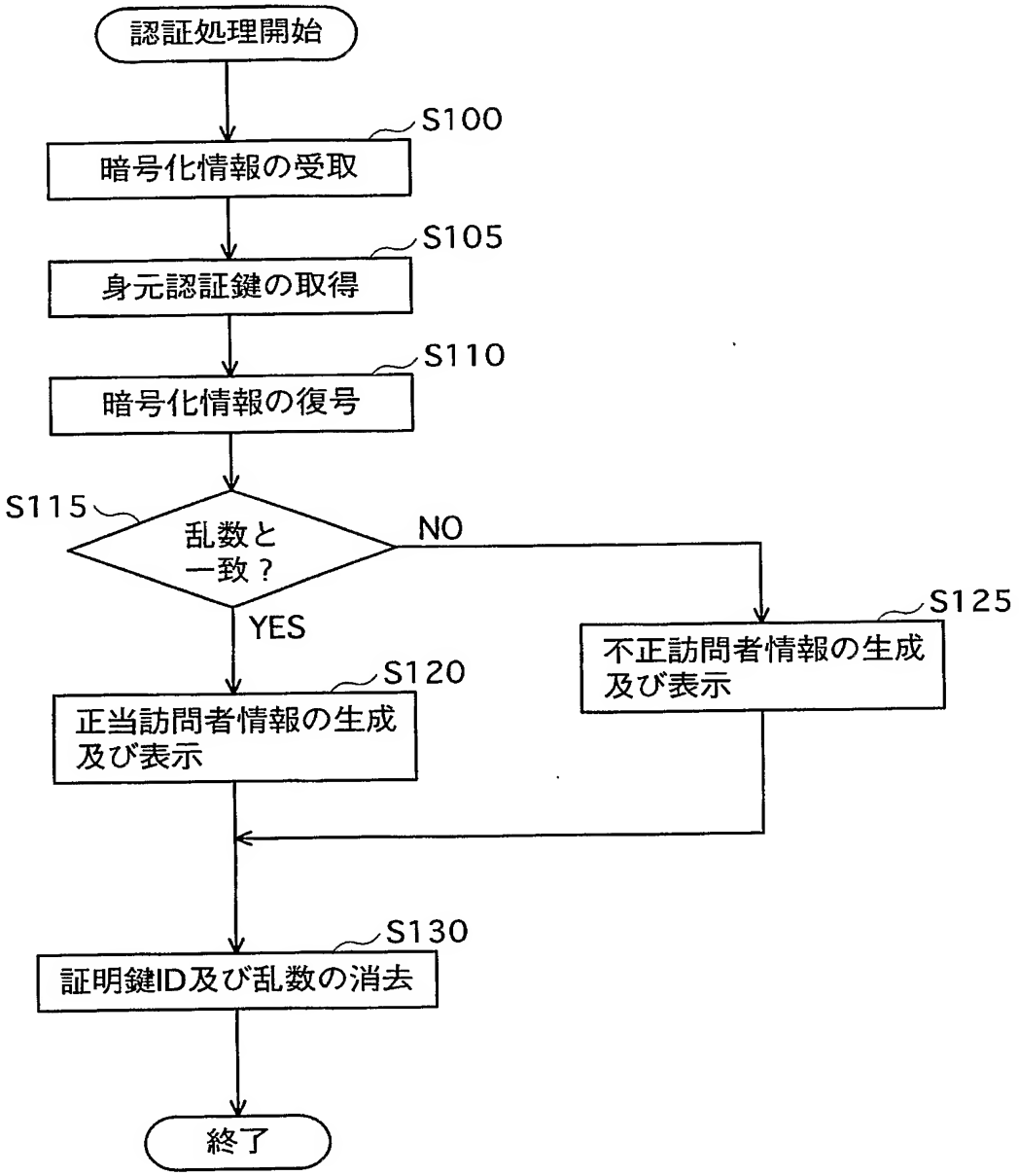
T100

認証鍵ID	身元認証鍵
ID 1	SK 1
ID 2	SK 2
ID 3	SK 3
・ ・ ・	・ ・ ・

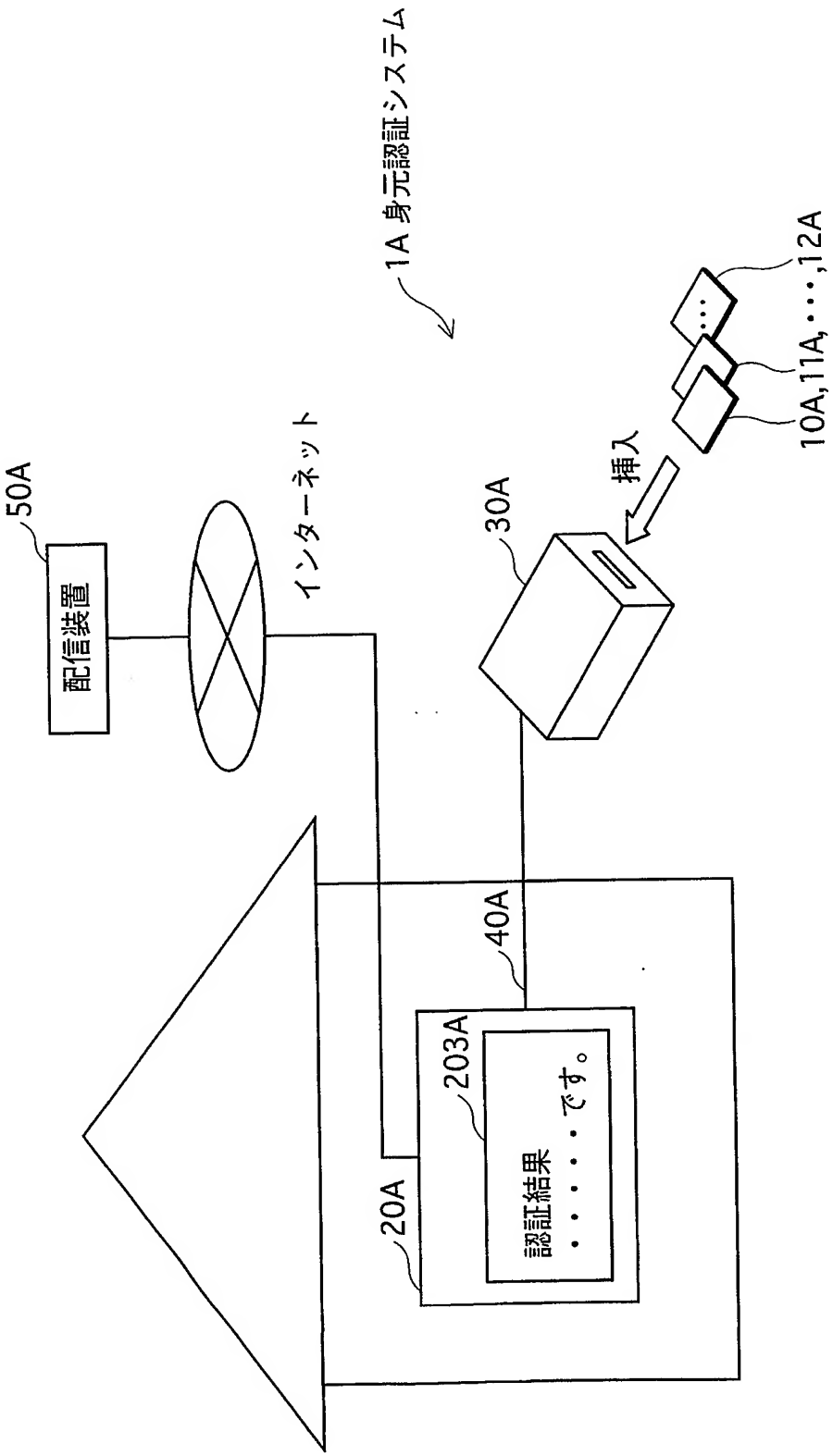
【図５】


ユーザ端末 20
カードリーダ 30
認証カード 10
S5
認証カードの挿入検知
S10
検知情報及びID要求情報の生成
S15
証明鍵IDの取得
S20
証明鍵IDの受取
S25
証明鍵ID及び検知情報の出力
S30
証明鍵IDの記憶
S35
乱数の生成
S40
乱数の出力
S45
乱数の受取
S50
暗号化情報の生成
S55
暗号化情報の出力
S60
認証処理

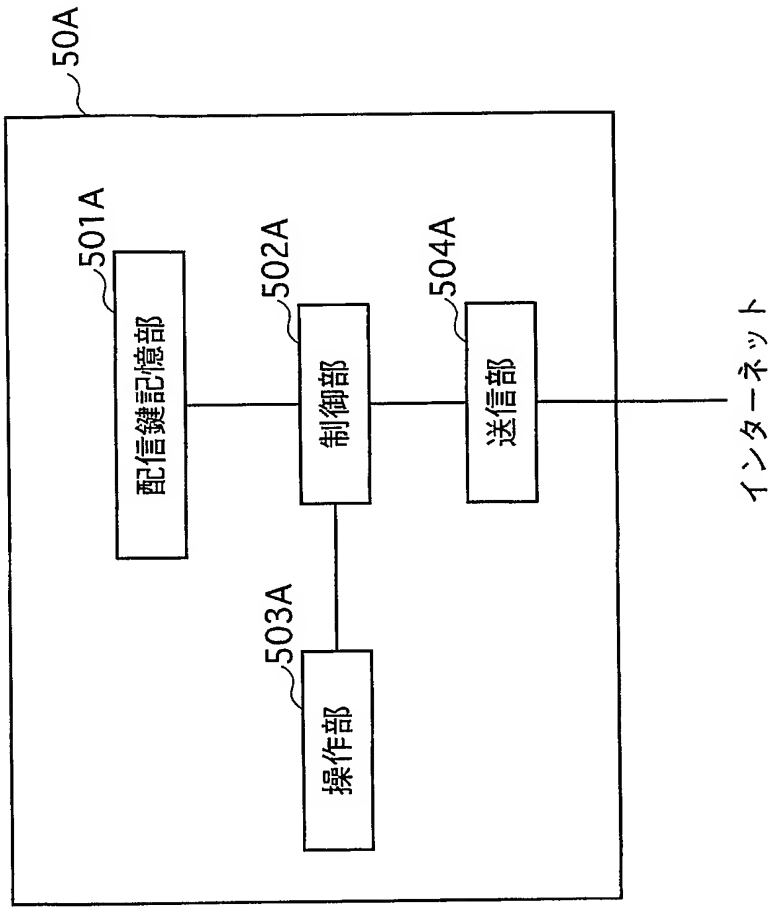
【図６】


認証処理開始
S100
暗号化情報の受取
S105
身元認証鍵の取得
S110
暗号化情報の復号
S115
乱数と
一致？
NO
YES
S120
正当訪問者情報の生成
及び表示
S125
不正訪問者情報の生成
及び表示
S130
証明鍵ID及び乱数の消去
終了

【図７】


1A 身元認証システム
10A,11A,・・・,12A
挿入
30A
50A
配信装置
インターネット
40A
203A
認証結果
・・・・・・です。
20A

【図８】

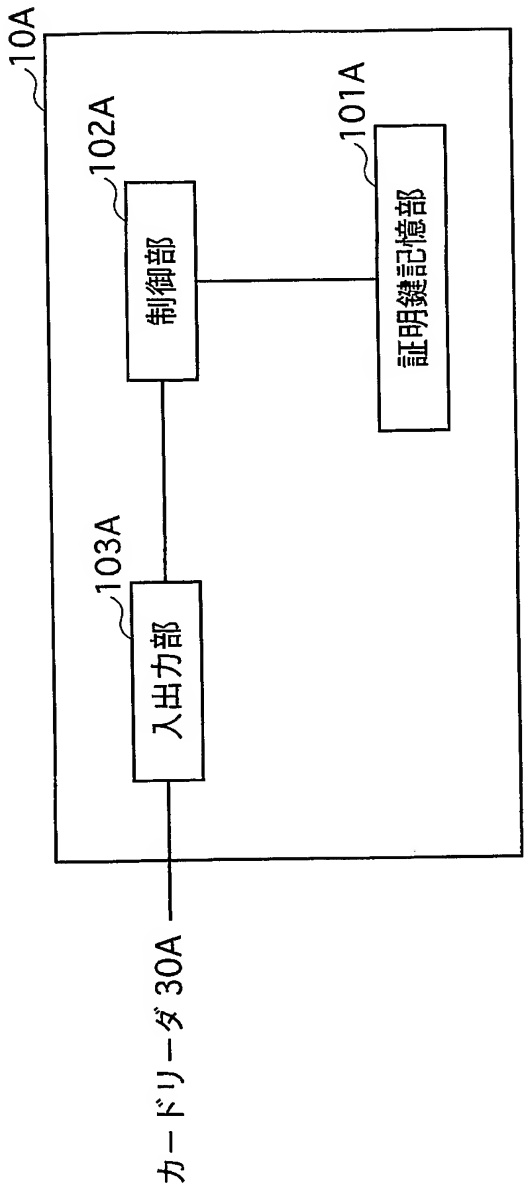


【図９】

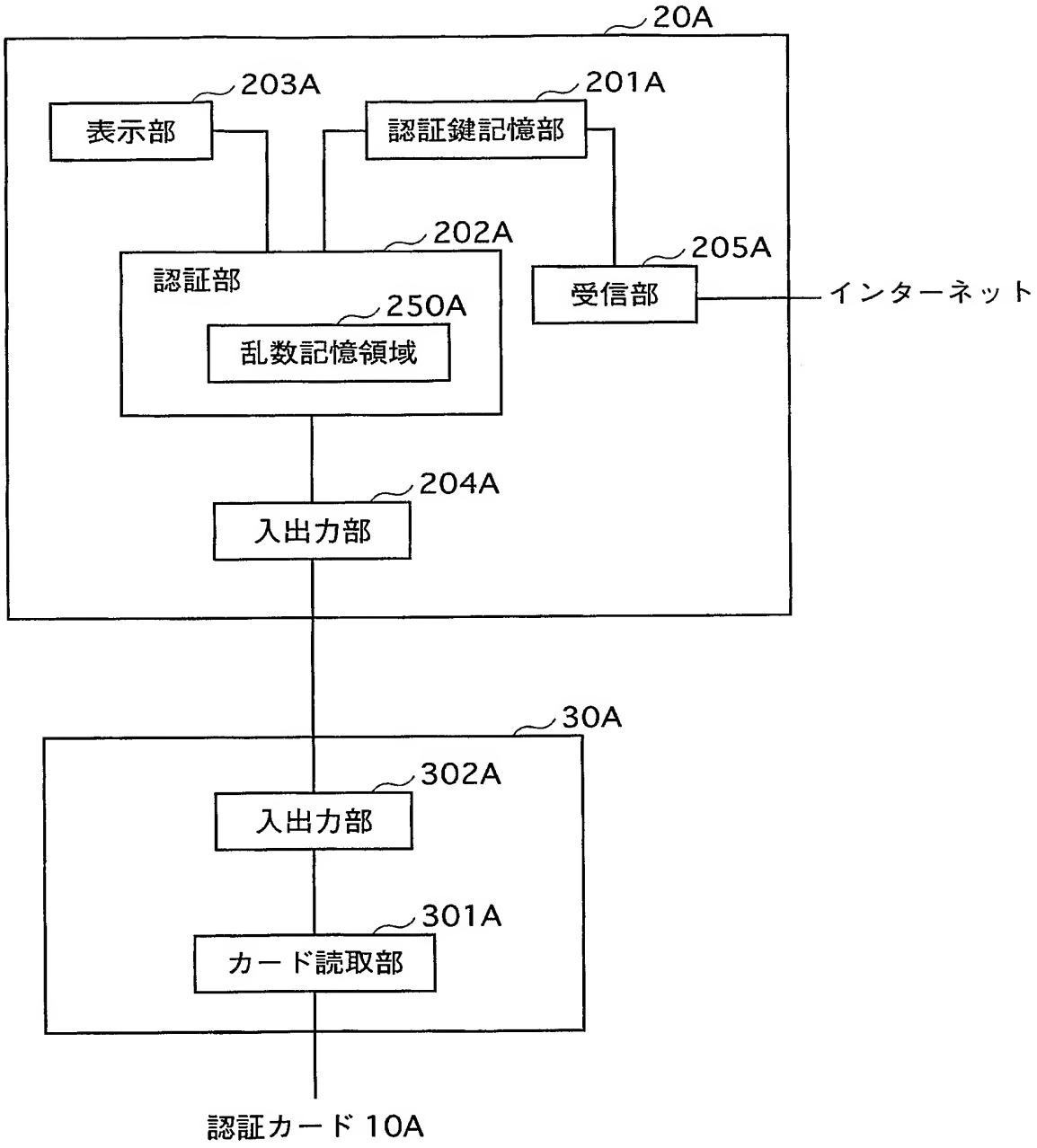
T200

訪問者ID	身元認証鍵
VID 1	SK 1
VID 2	SK 2
・ ・ ・	・ ・ ・

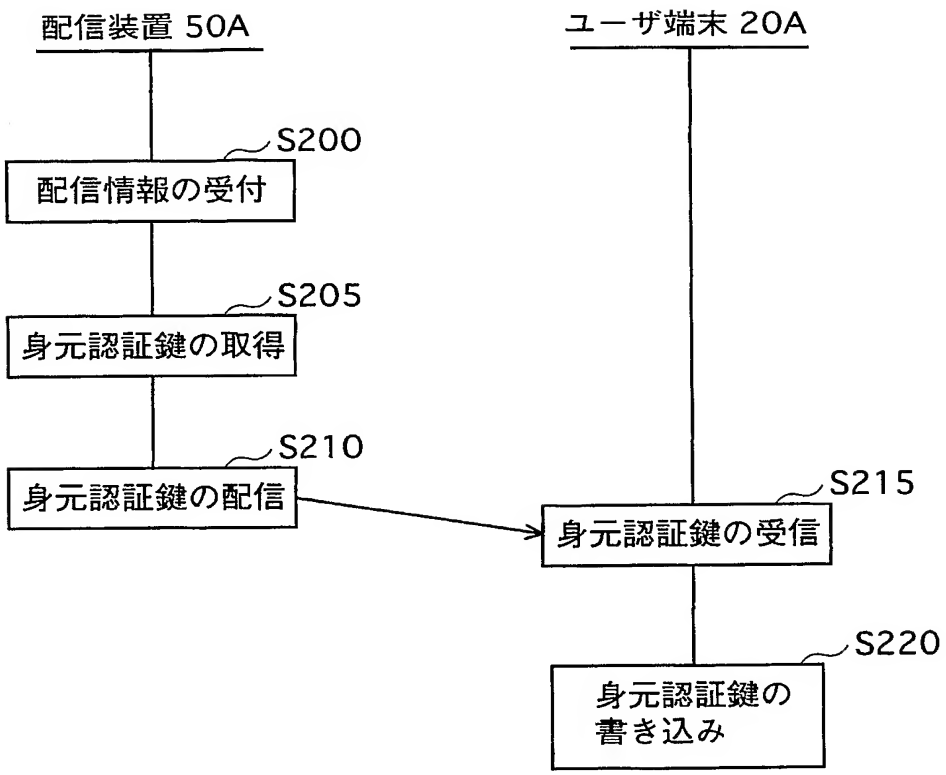
【図１０】



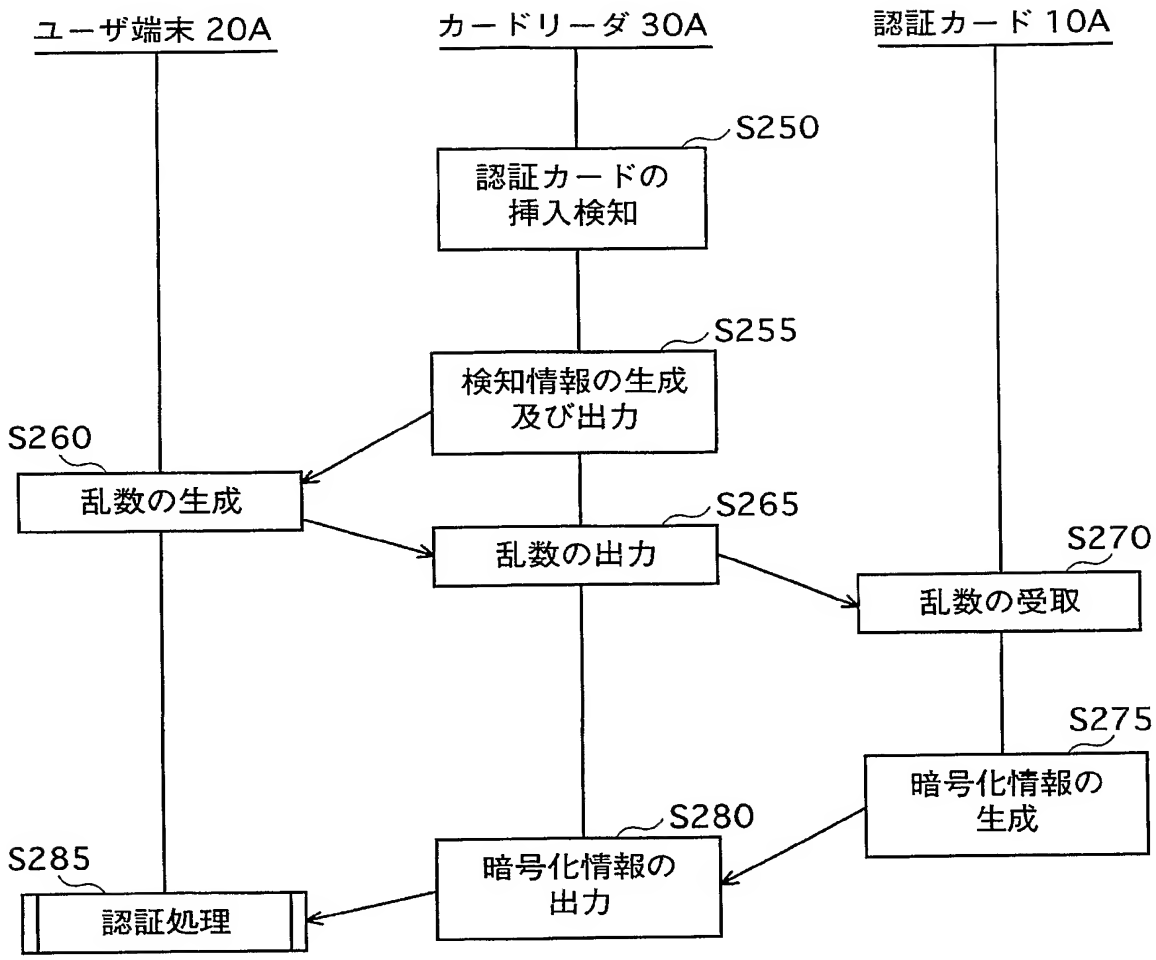
【図１１】


20A
203A
表示部
201A
認証鍵記憶部
202A
認証部
250A
乱数記憶領域
205A
受信部
インターネット
204A
入出力部
30A
302A
入出力部
301A
カード読取部
認証カード 10A

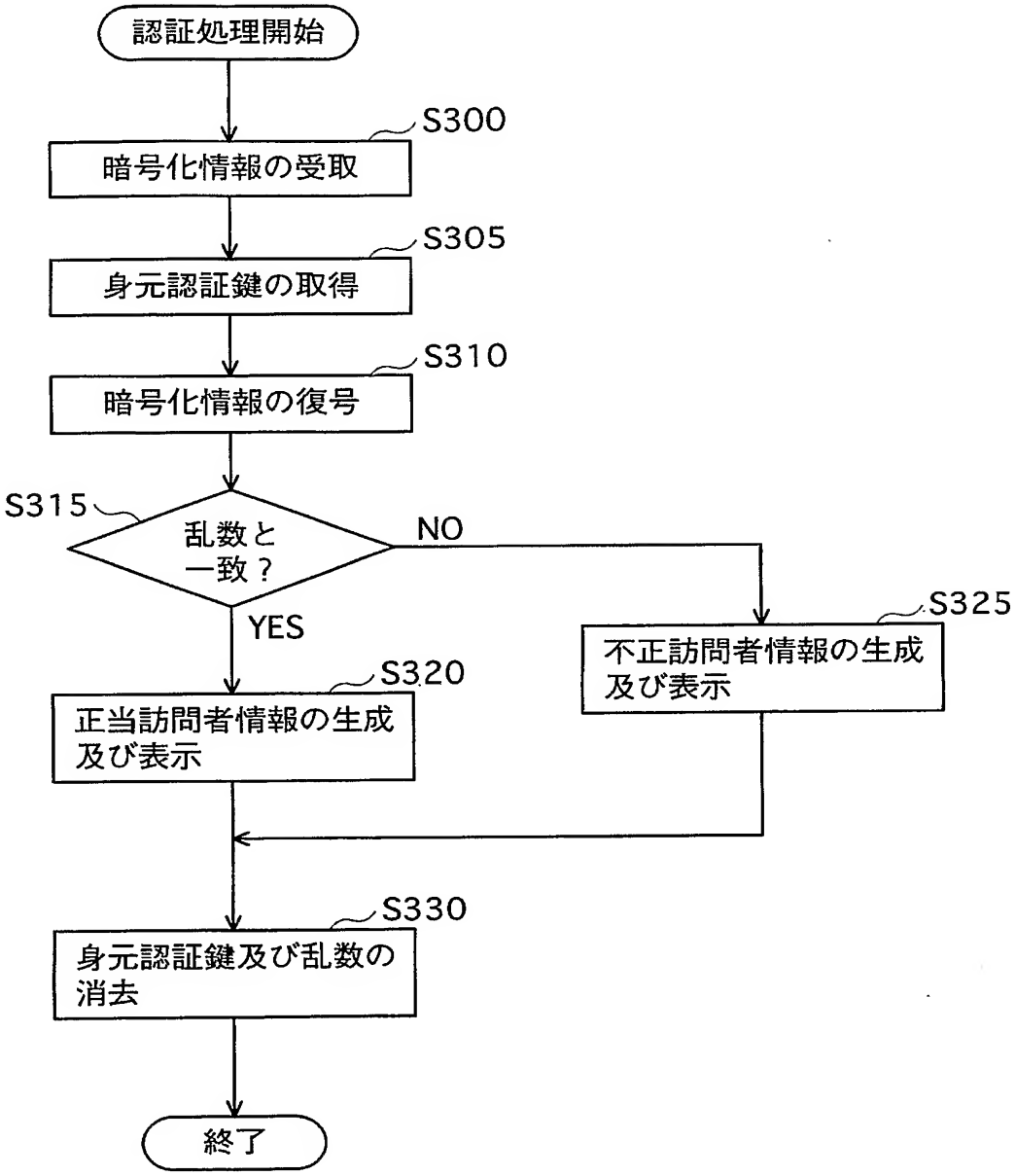
【図１２】


配信装置 50A
ユーザ端末 20A
S200
配信情報の受付
S205
身元認証鍵の取得
S210
身元認証鍵の配信
S215
身元認証鍵の受信
S220
身元認証鍵の
書き込み

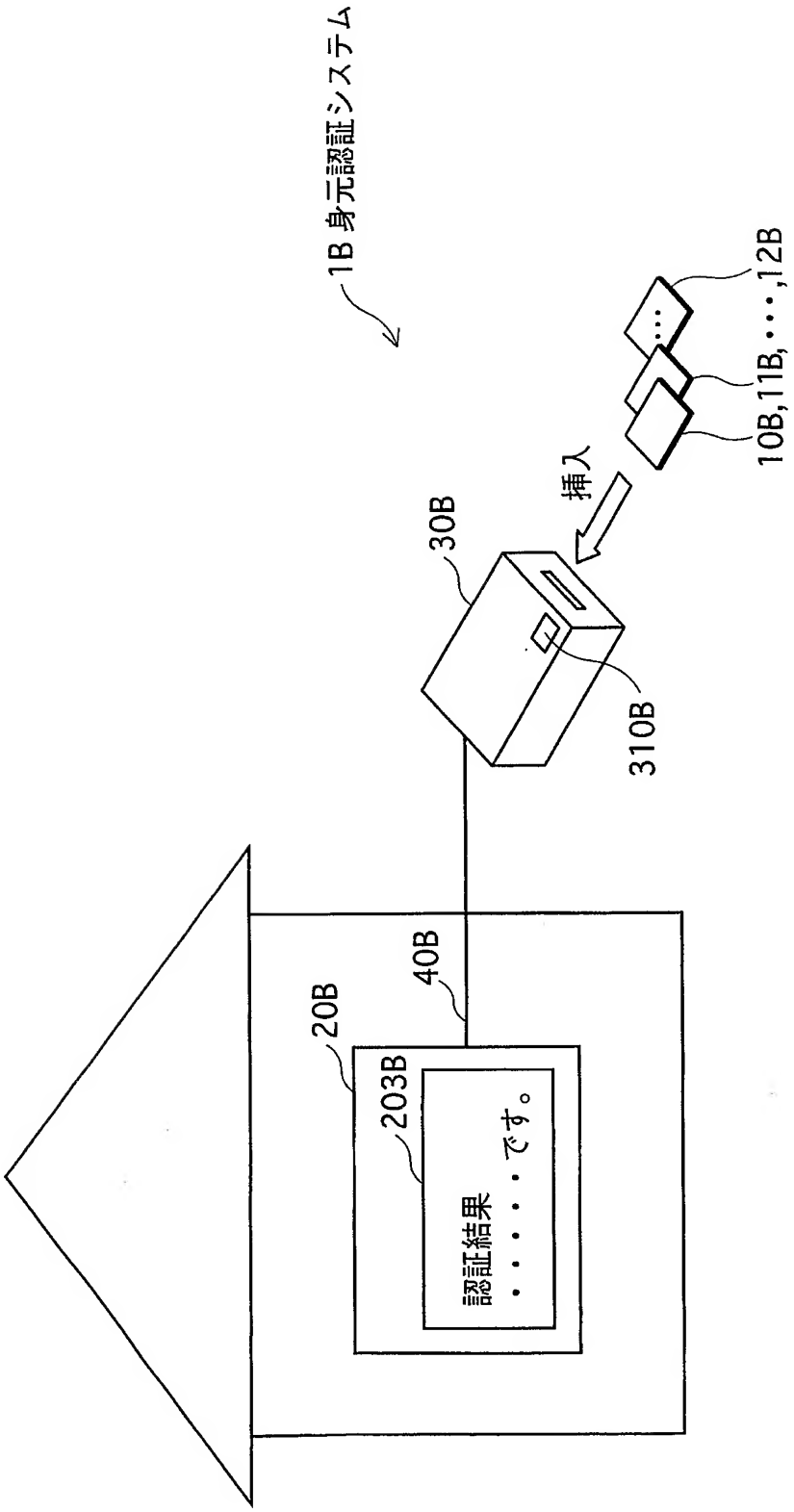
【図１３】


ユーザ端末 20A
カードリーダ 30A
認証カード 10A
S250
認証カードの挿入検知
S255
検知情報の生成及び出力
S260
乱数の生成
S265
乱数の出力
S270
乱数の受取
S275
暗号化情報の生成
S280
暗号化情報の出力
S285
認証処理

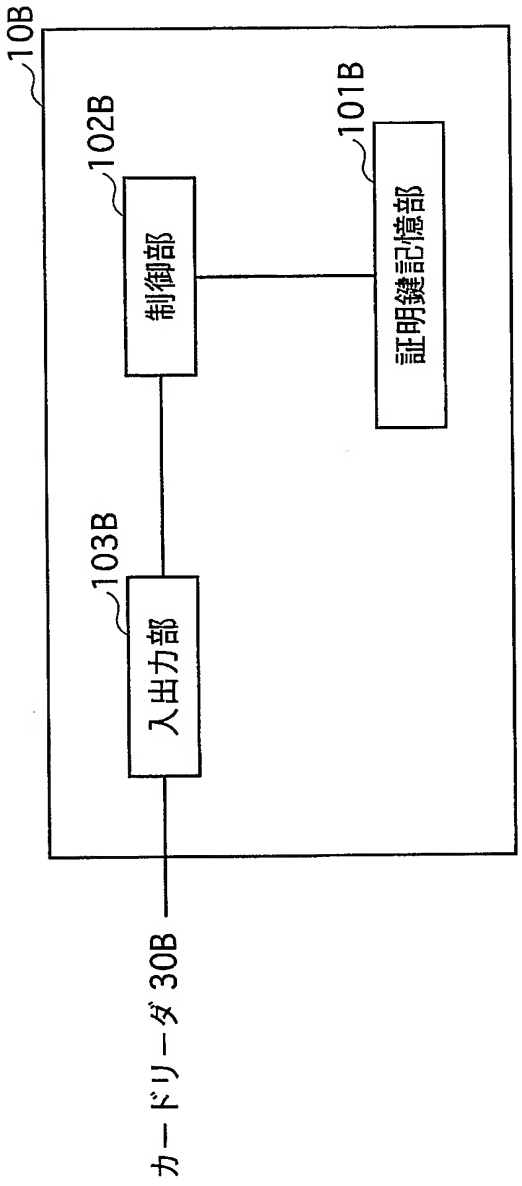
【図１４】


認証処理開始
S300
暗号化情報の受取
S305
身元認証鍵の取得
S310
暗号化情報の復号
S315
乱数と
一致？
NO
YES
S325
不正訪問者情報の生成
及び表示
S320
正当訪問者情報の生成
及び表示
S330
身元認証鍵及び乱数の
消去
終了

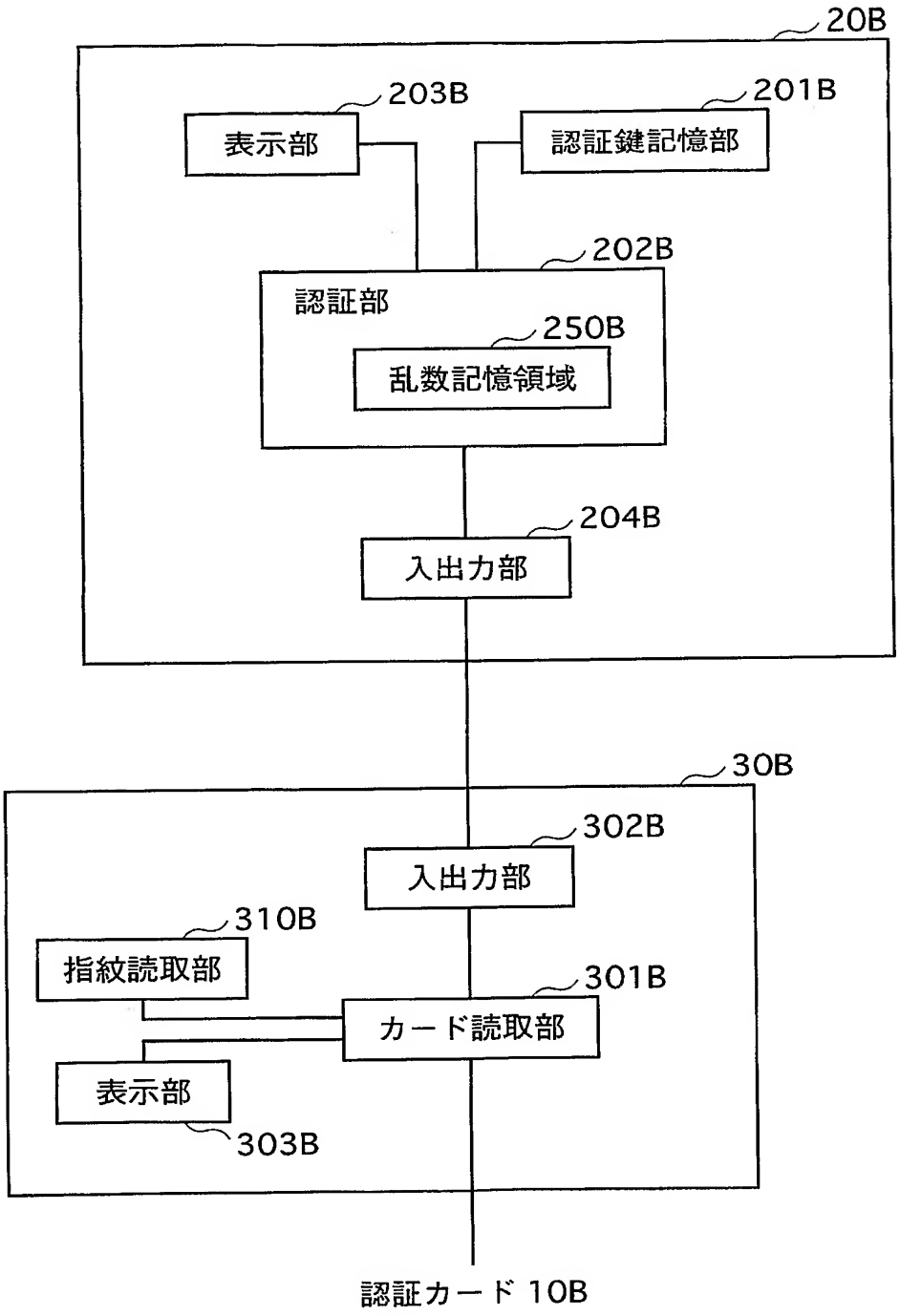
【図１５】



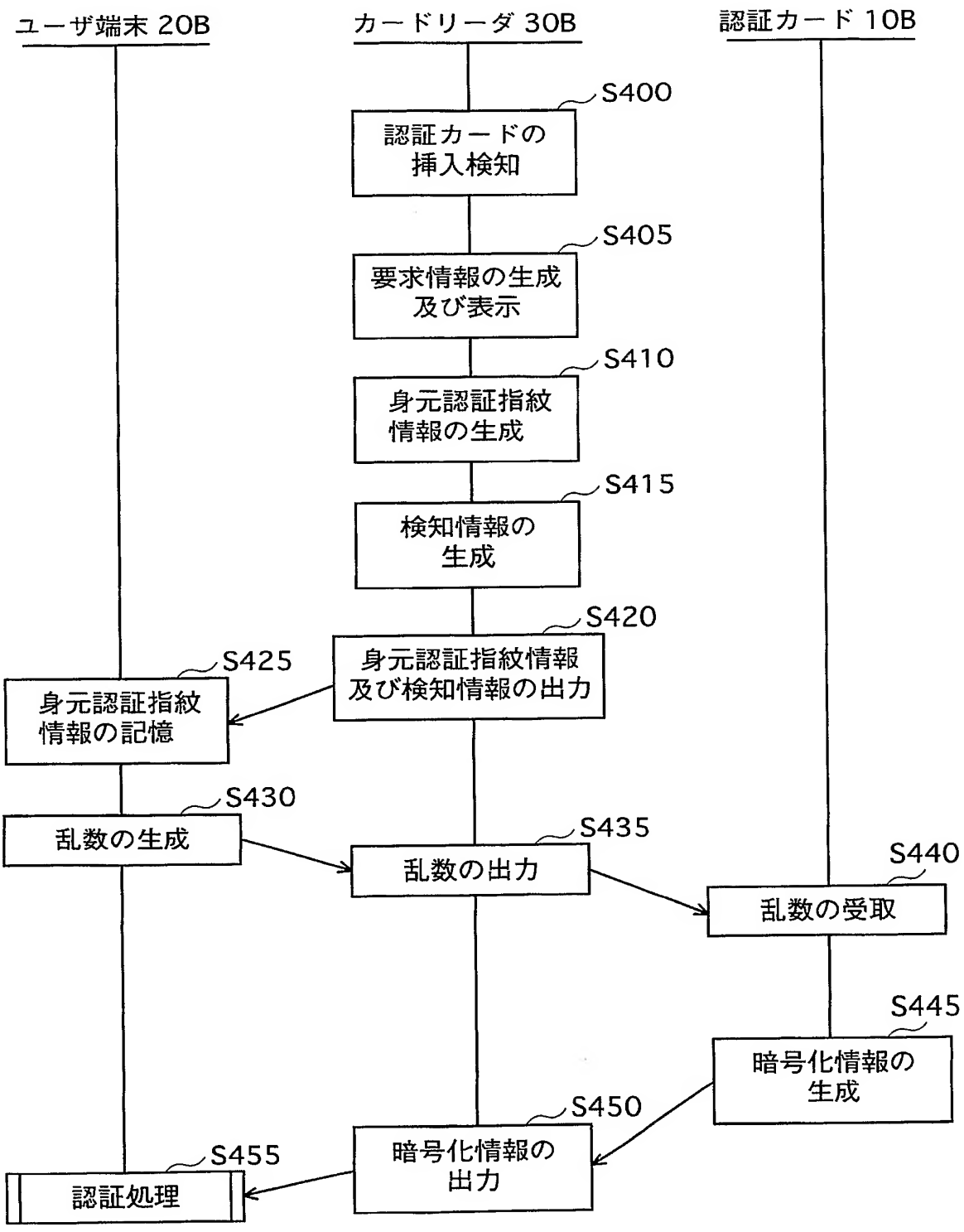
【図１６】



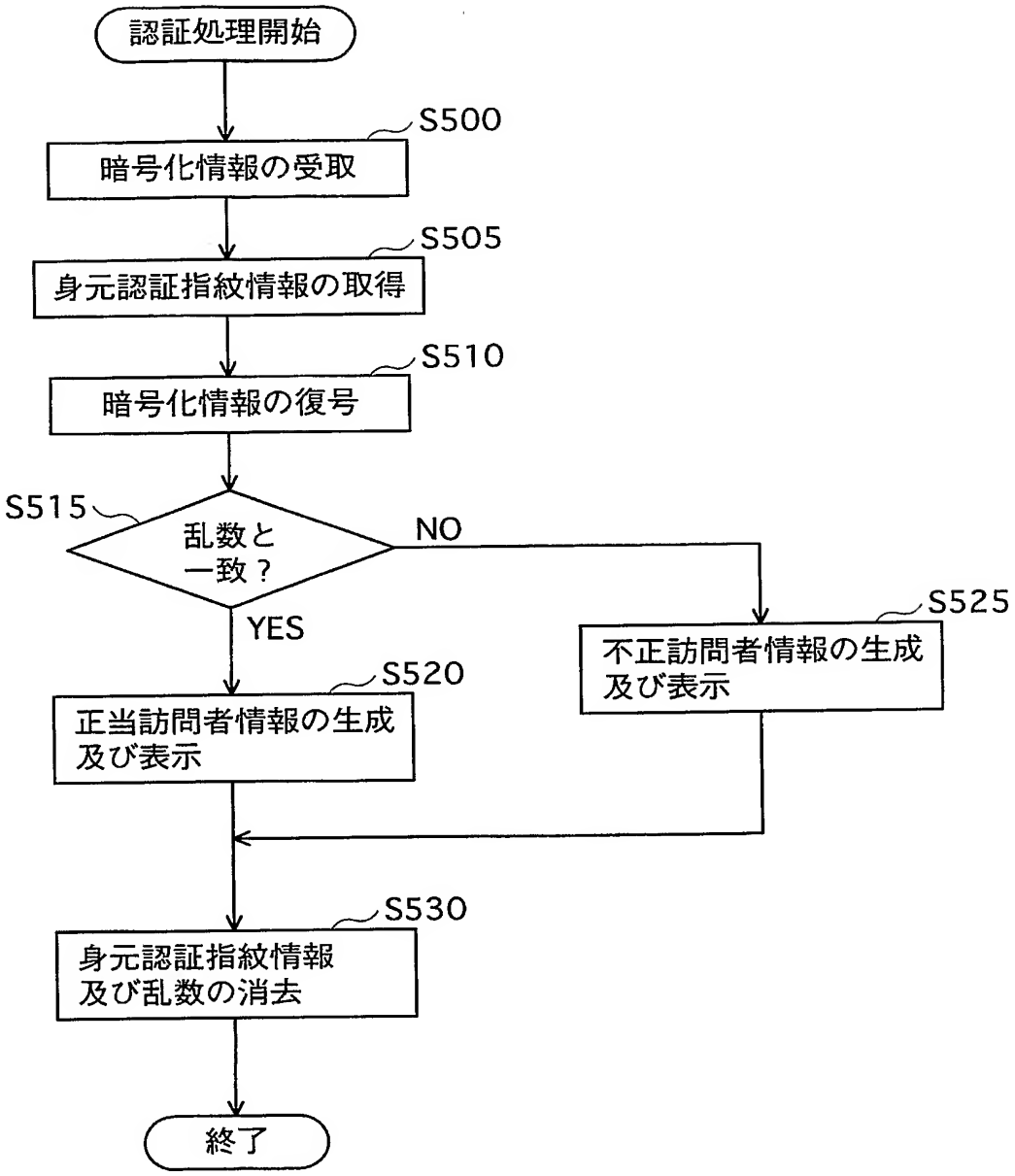
【図１７】


20B
203B
表示部
201B
認証鍵記憶部
202B
認証部
250B
乱数記憶領域
204B
入出力部
30B
302B
入出力部
310B
指紋読取部
301B
カード読取部
表示部
303B
認証カード 10B

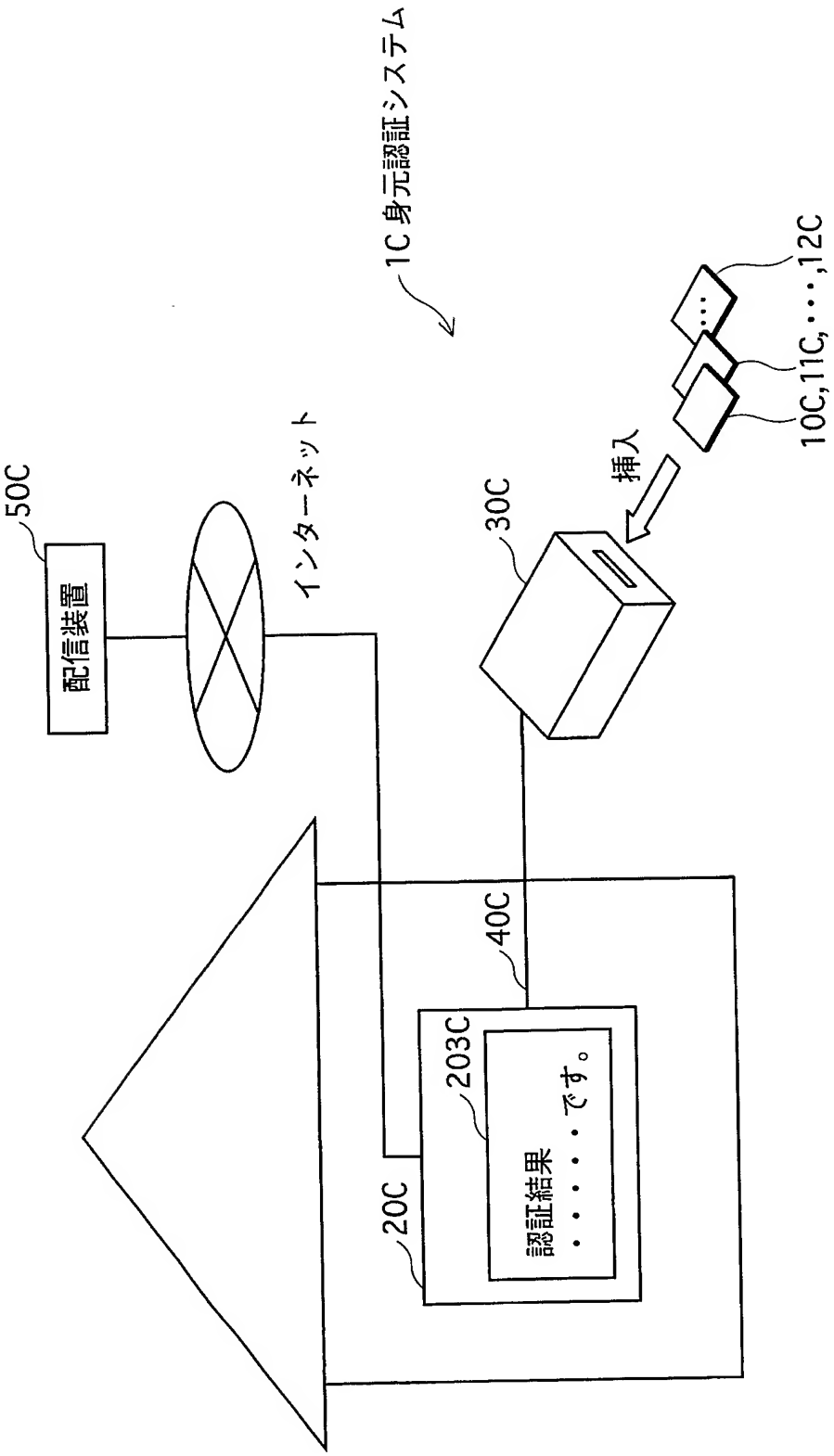
【図１８】


ユーザ端末 20B
カードリーダ 30B
認証カード 10B
S400
認証カードの挿入検知
S405
要求情報の生成及び表示
S410
身元認証指紋情報の生成
S415
検知情報の生成
S420
身元認証指紋情報及び検知情報の出力
S425
身元認証指紋情報の記憶
S430
乱数の生成
S435
乱数の出力
S440
乱数の受取
S445
暗号化情報の生成
S450
暗号化情報の出力
S455
認証処理

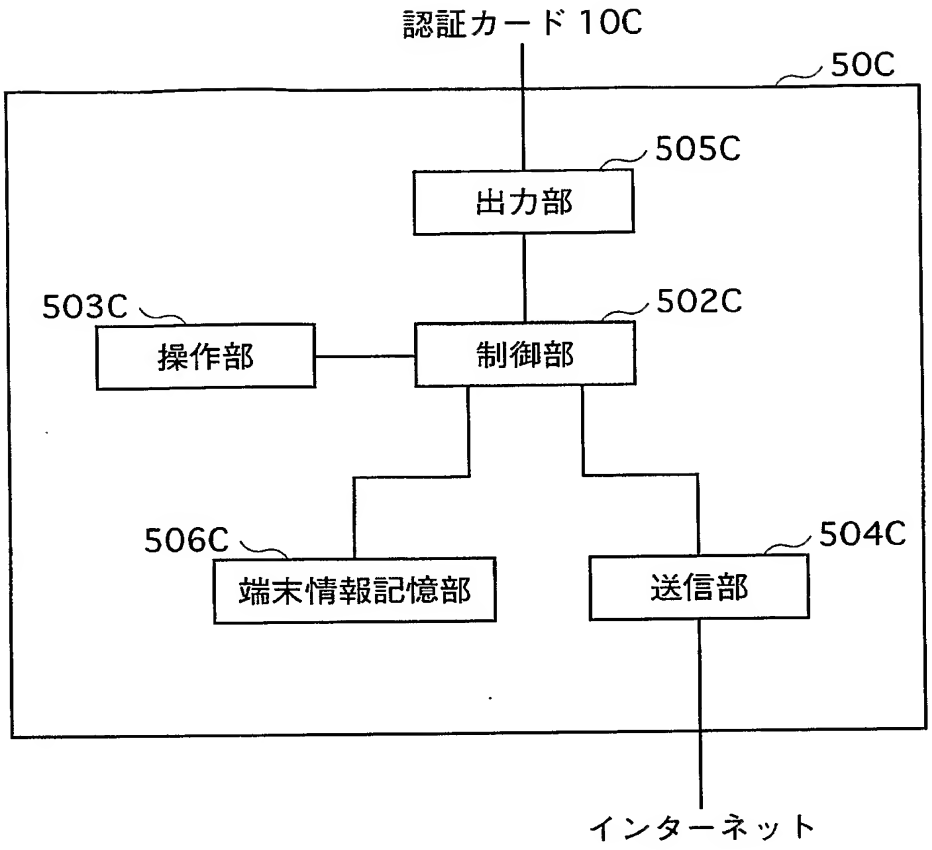
【図１９】


認証処理開始
S500
暗号化情報の受取
S505
身元認証指紋情報の取得
S510
暗号化情報の復号
S515
乱数と
一致？
NO
YES
S520
正当訪問者情報の生成
及び表示
S525
不正訪問者情報の生成
及び表示
S530
身元認証指紋情報
及び乱数の消去
終了

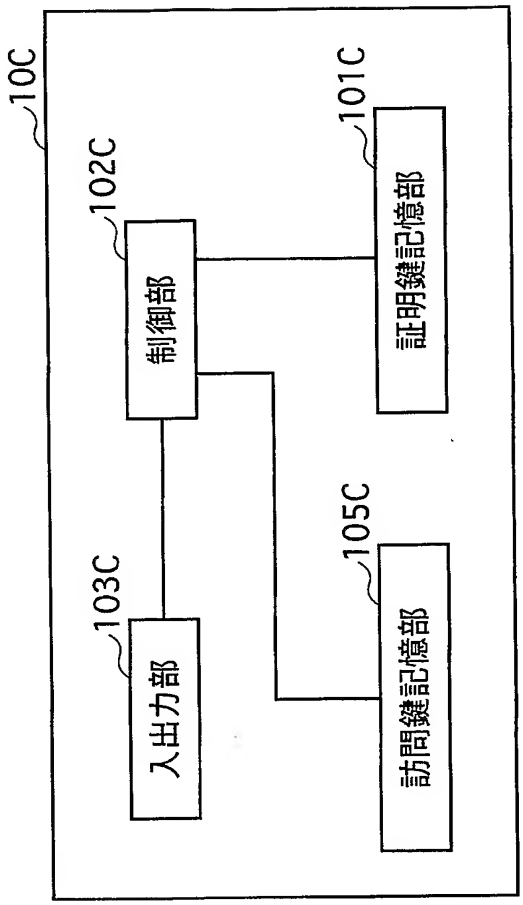
【図２０】


1C 身元認証システム
10C,11C,・・・,12C
挿入
30C
50C
配信装置
インターネット
40C
203C
認証結果
・・・・・です。
20C

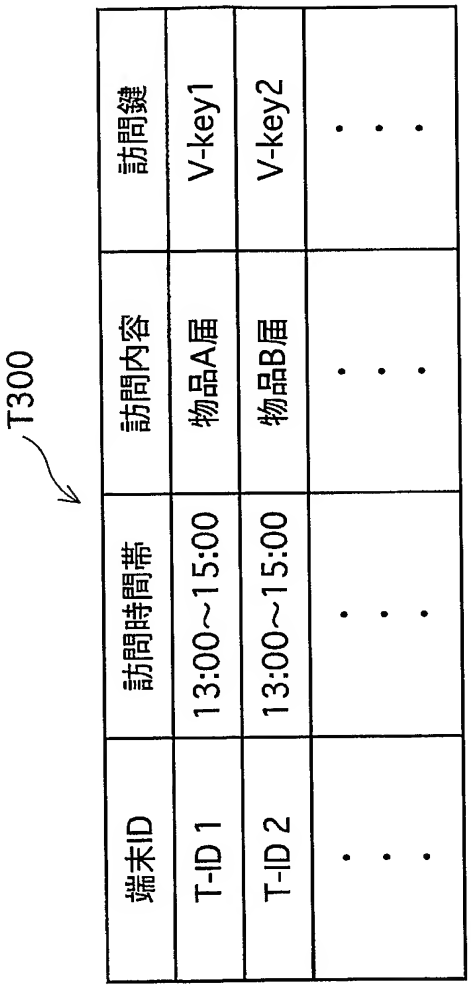
【図２１】


認証カード10C
50C
505C
出力部
503C
操作部
502C
制御部
506C
端末情報記憶部
504C
送信部
インターネット

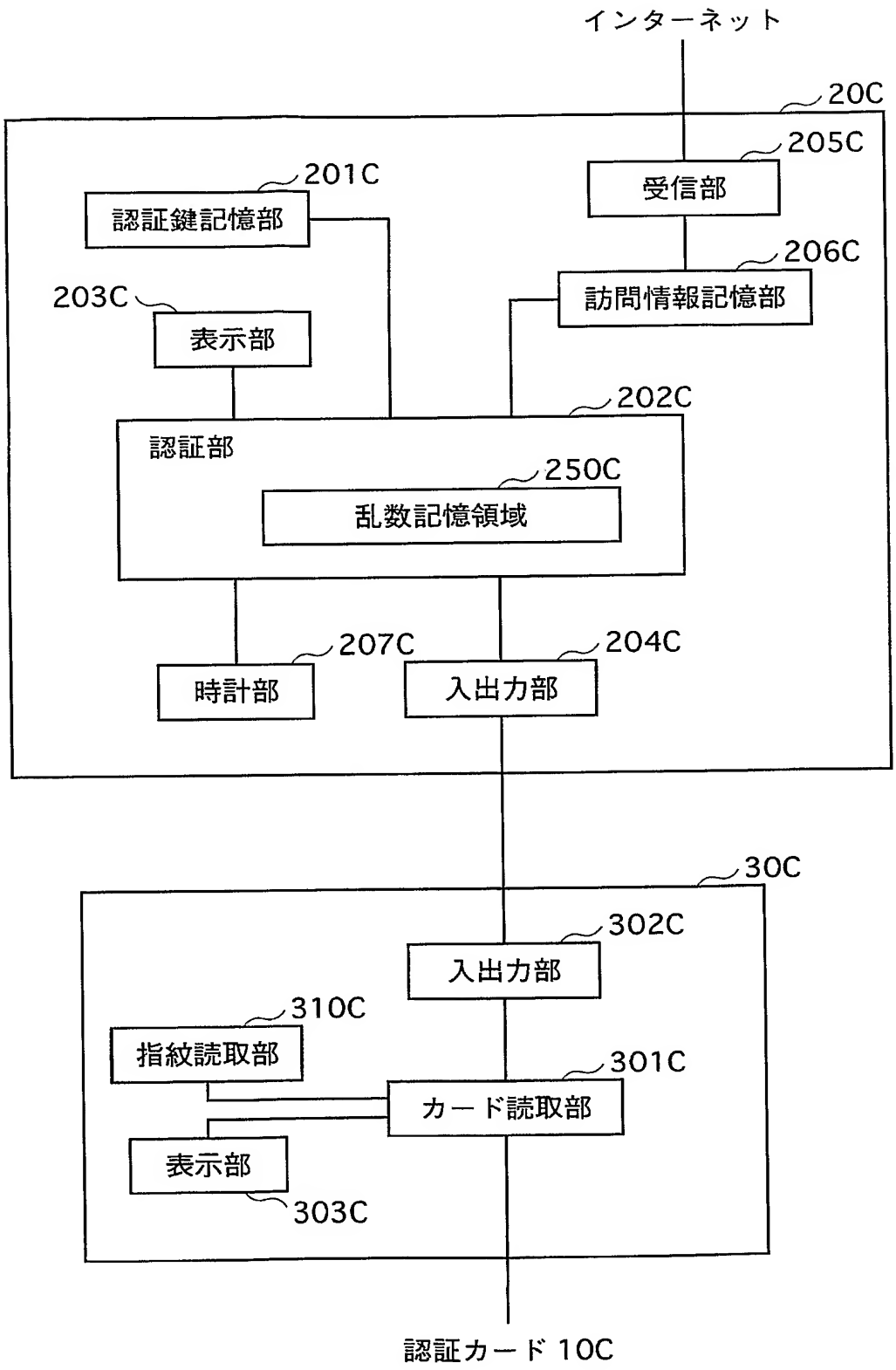
【図２２】



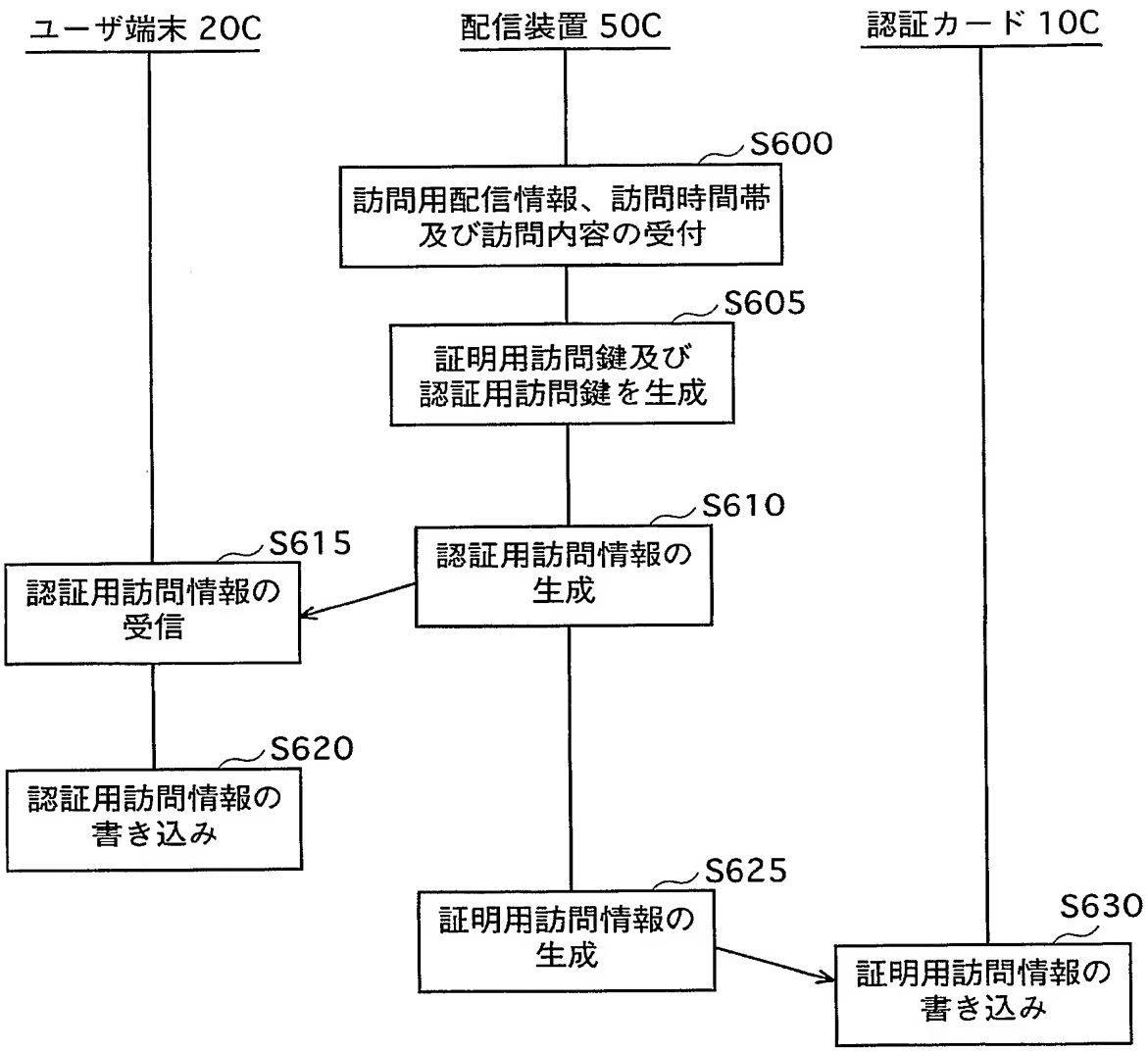
【図２３】


T300
端末ID
訪問時間帯
訪問内容
訪問鍵
T-ID 1
13:00～15:00
物品A届
V-key1
T-ID 2
13:00～15:00
物品B届
V-key2

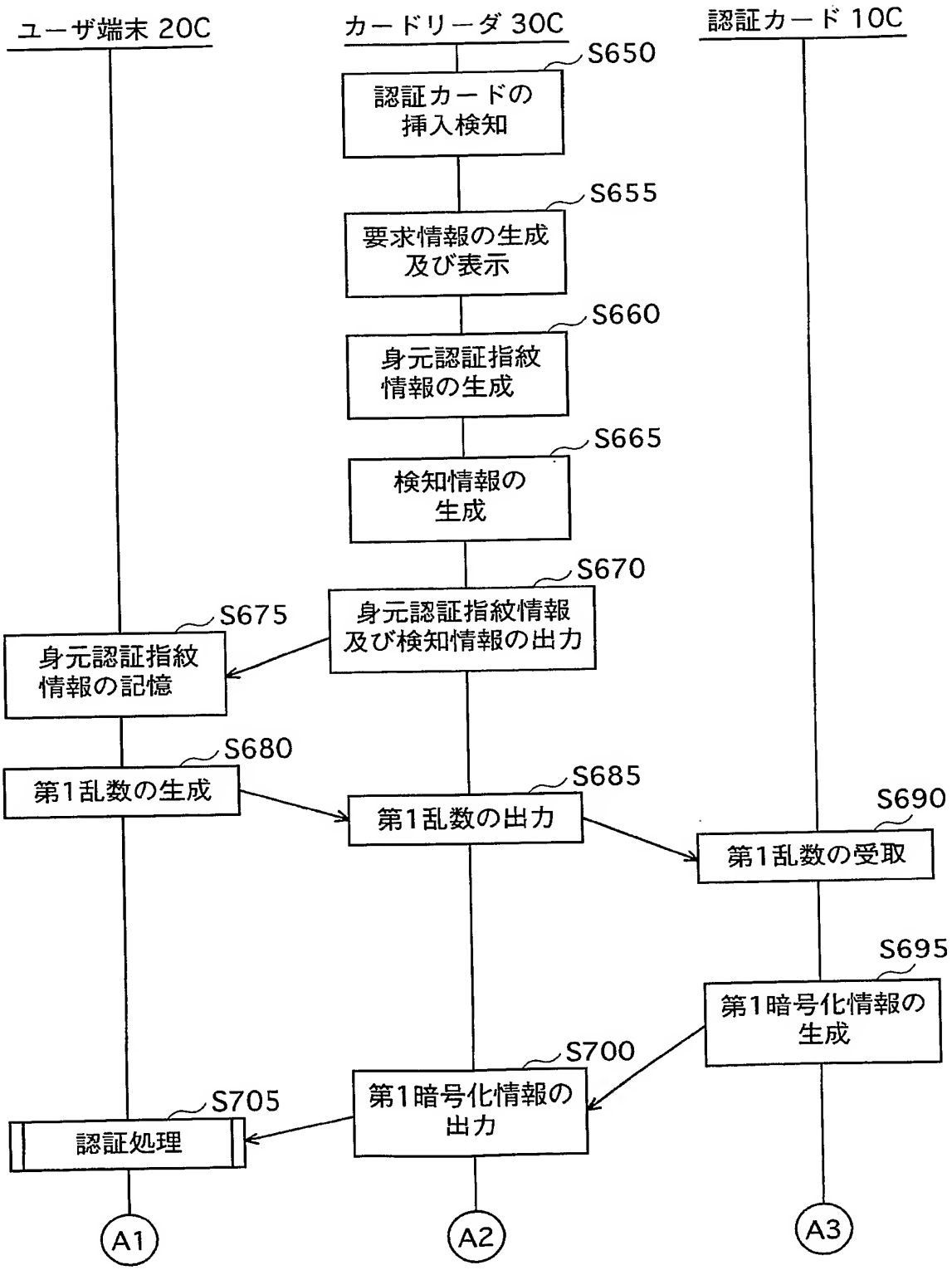
【図２４】


インターネット
20C
205C
受信部
201C
認証鍵記憶部
206C
訪問情報記憶部
203C
表示部
202C
認証部
250C
乱数記憶領域
207C
時計部
204C
入出力部
30C
302C
入出力部
310C
指紋読取部
301C
カード読取部
表示部
303C
認証カード 10C

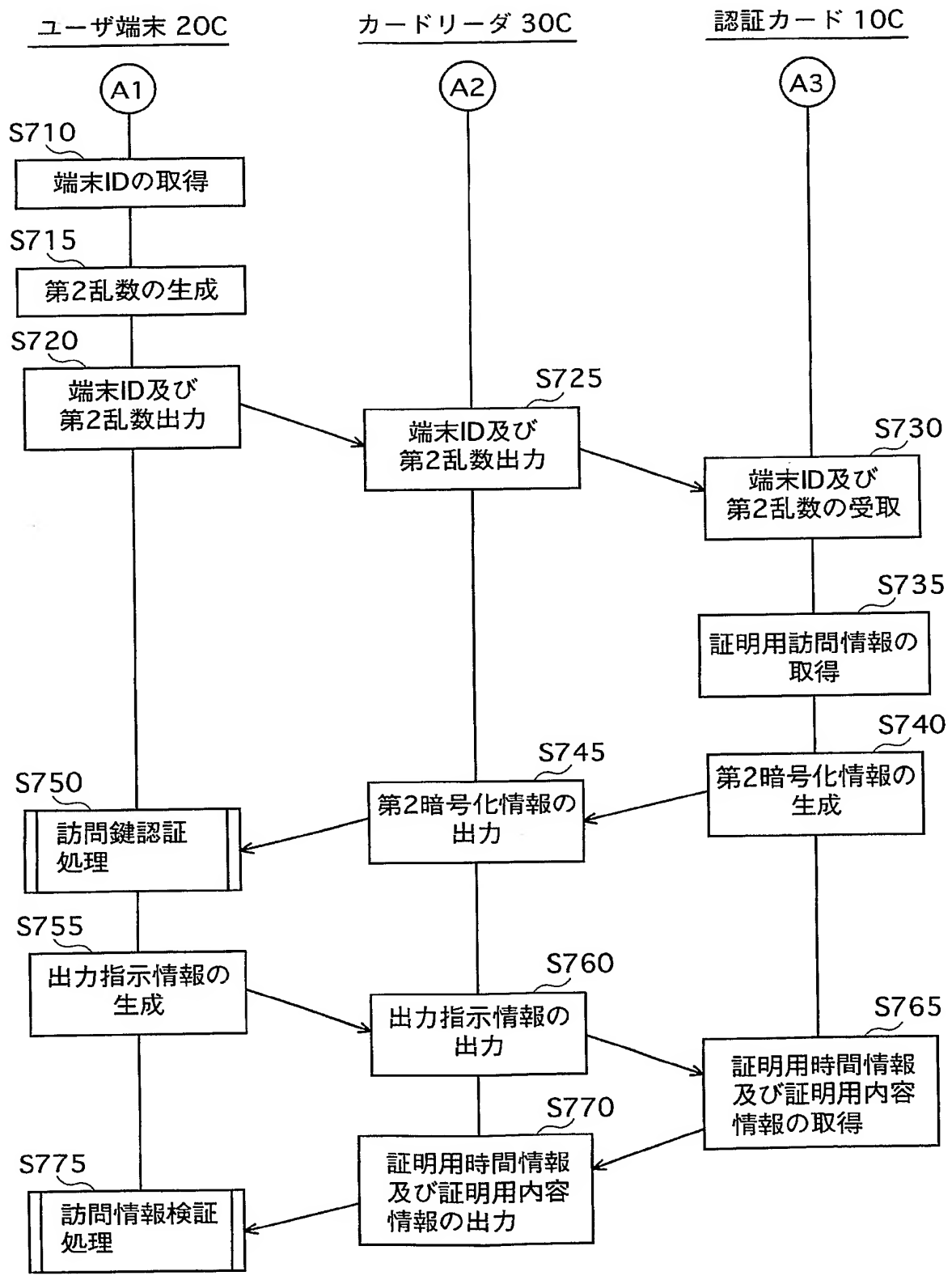
【図２５】


ユーザ端末 20C
配信装置 50C
認証カード 10C
S600
訪問用配信情報、訪問時間帯及び訪問内容の受付
S605
証明用訪問鍵及び認証用訪問鍵を生成
S610
認証用訪問情報の生成
S615
認証用訪問情報の受信
S620
認証用訪問情報の書き込み
S625
証明用訪問情報の生成
S630
証明用訪問情報の書き込み

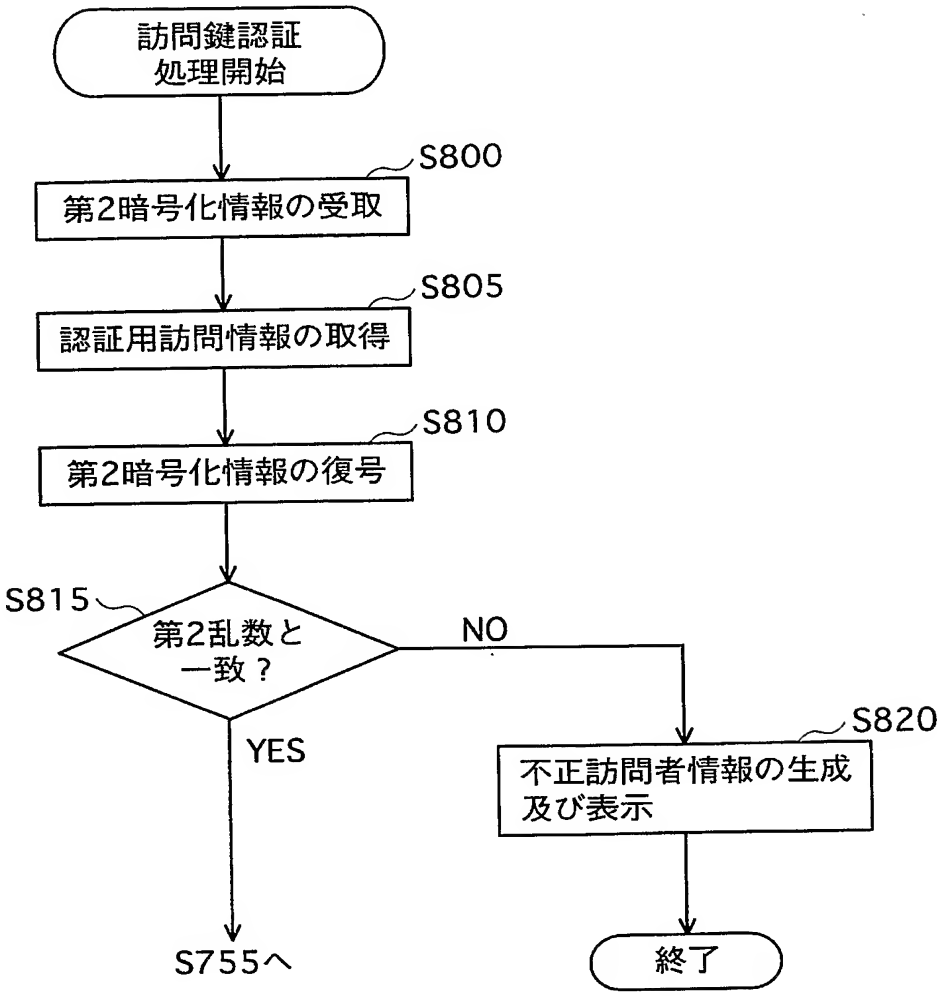
【図２６】


ユーザ端末 20C
カードリーダ 30C
認証カード 10C
S650
認証カードの挿入検知
S655
要求情報の生成及び表示
S660
身元認証指紋情報の生成
S665
検知情報の生成
S670
身元認証指紋情報及び検知情報の出力
S675
身元認証指紋情報の記憶
S680
第1乱数の生成
S685
第1乱数の出力
S690
第1乱数の受取
S695
第1暗号化情報の生成
S700
第1暗号化情報の出力
S705
認証処理
A1
A2
A3

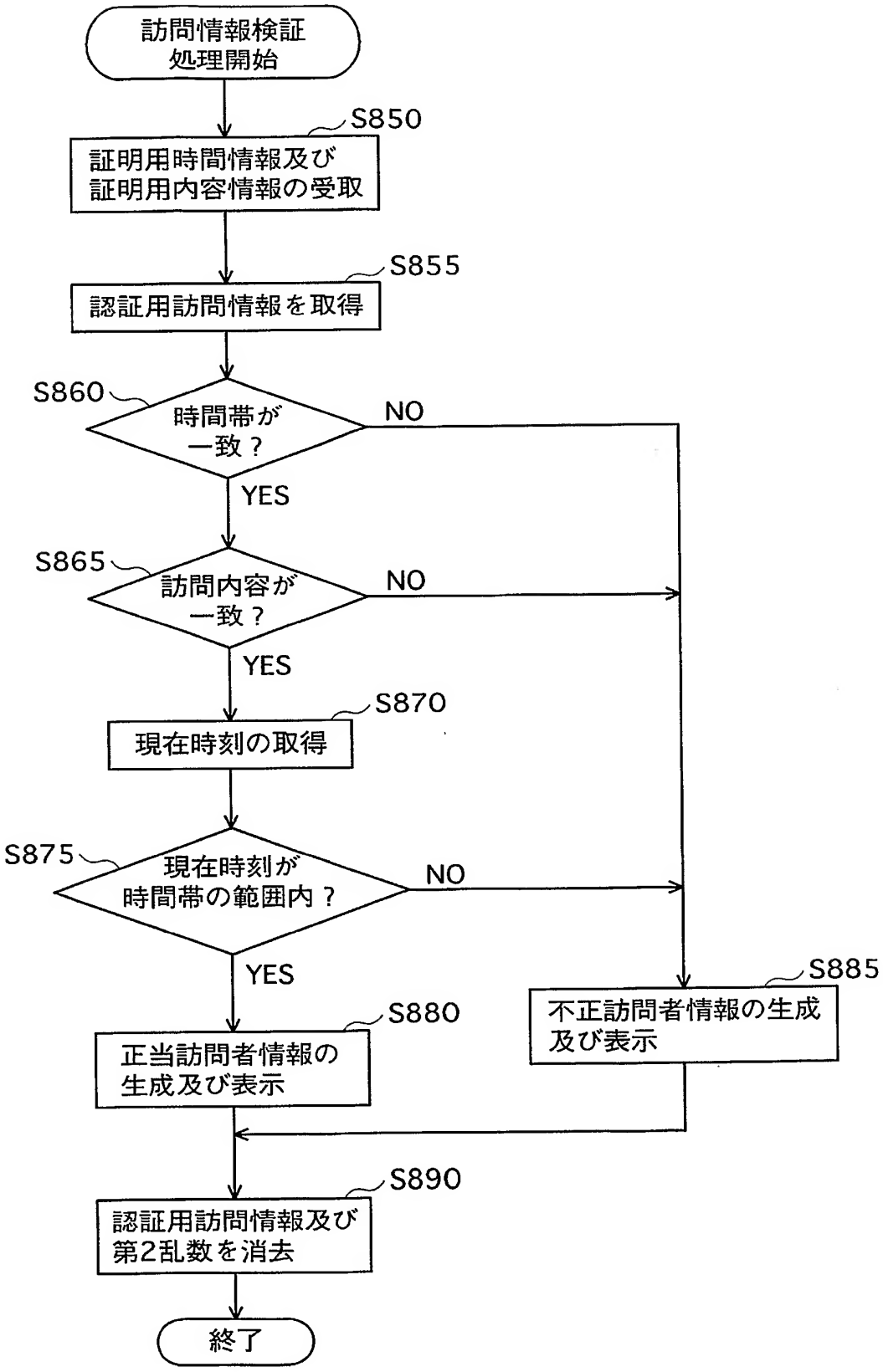
【図２７】


ユーザ端末 20C
カードリーダ 30C
認証カード 10C
A1
A2
A3
S710
端末IDの取得
S715
第2乱数の生成
S720
端末ID及び第2乱数出力
S725
端末ID及び第2乱数出力
S730
端末ID及び第2乱数の受取
S735
証明用訪問情報の取得
S740
第2暗号化情報の生成
S745
第2暗号化情報の出力
S750
訪問鍵認証処理
S755
出力指示情報の生成
S760
出力指示情報の出力
S765
証明用時間情報及び証明用内容情報の取得
S770
証明用時間情報及び証明用内容情報の出力
S775
訪問情報検証処理

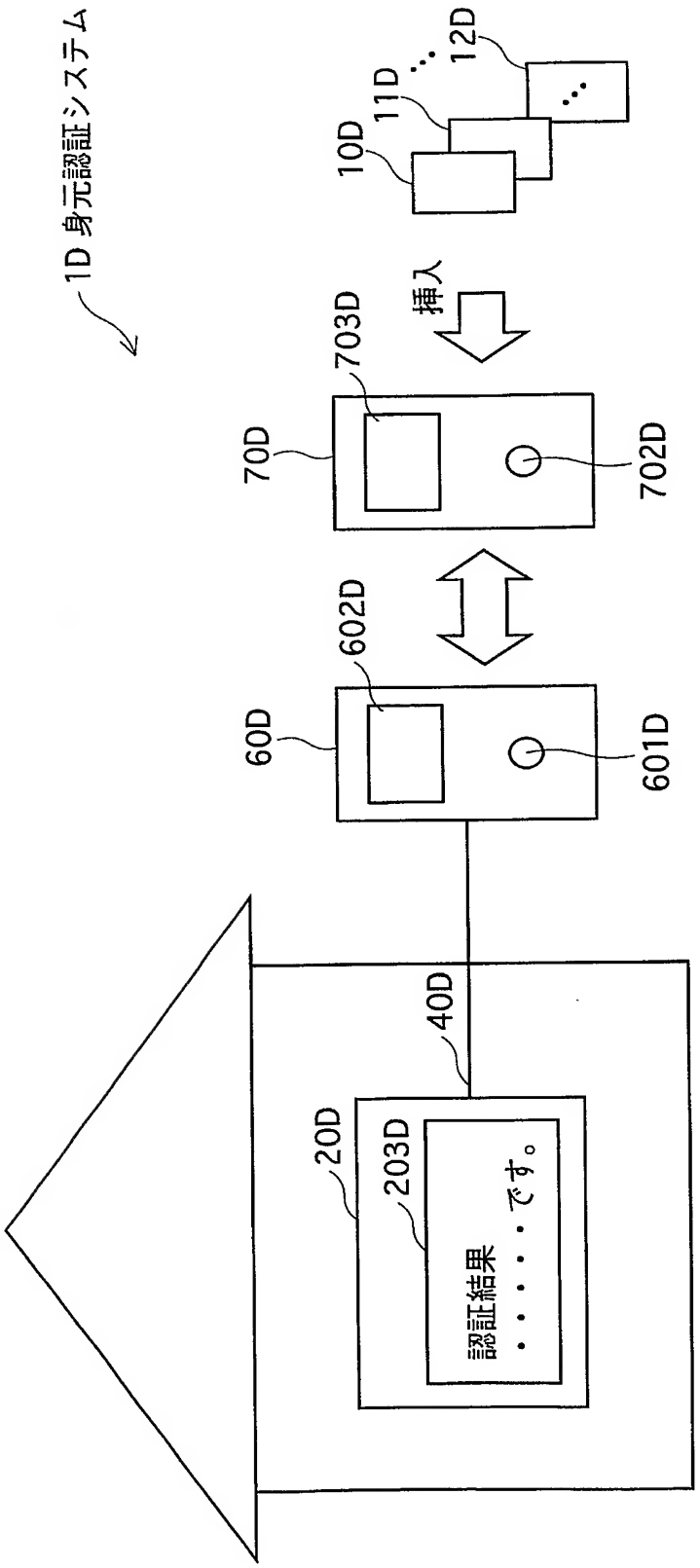
【図２８】


訪問鍵認証
処理開始
S800
第2暗号化情報の受取
S805
認証用訪問情報の取得
S810
第2暗号化情報の復号
S815
第2乱数と
一致？
NO
YES
S820
不正訪問者情報の生成
及び表示
S755へ
終了

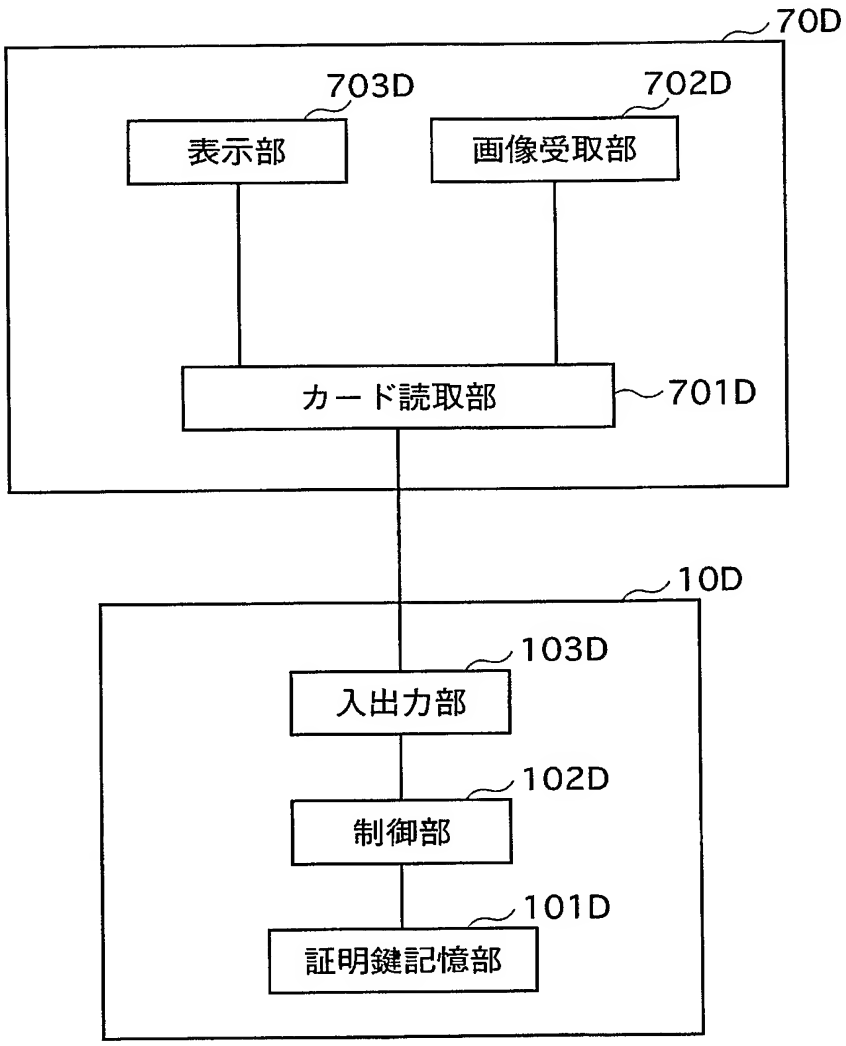
【図２９】


訪問情報検証
処理開始
S850
証明用時間情報及び
証明用内容情報の受取
S855
認証用訪問情報を取得
S860
時間帯が
一致？
NO
YES
S865
訪問内容が
一致？
NO
YES
S870
現在時刻の取得
S875
現在時刻が
時間帯の範囲内？
NO
YES
S880
正当訪問者情報の
生成及び表示
S885
不正訪問者情報の生成
及び表示
S890
認証用訪問情報及び
第2乱数を消去
終了

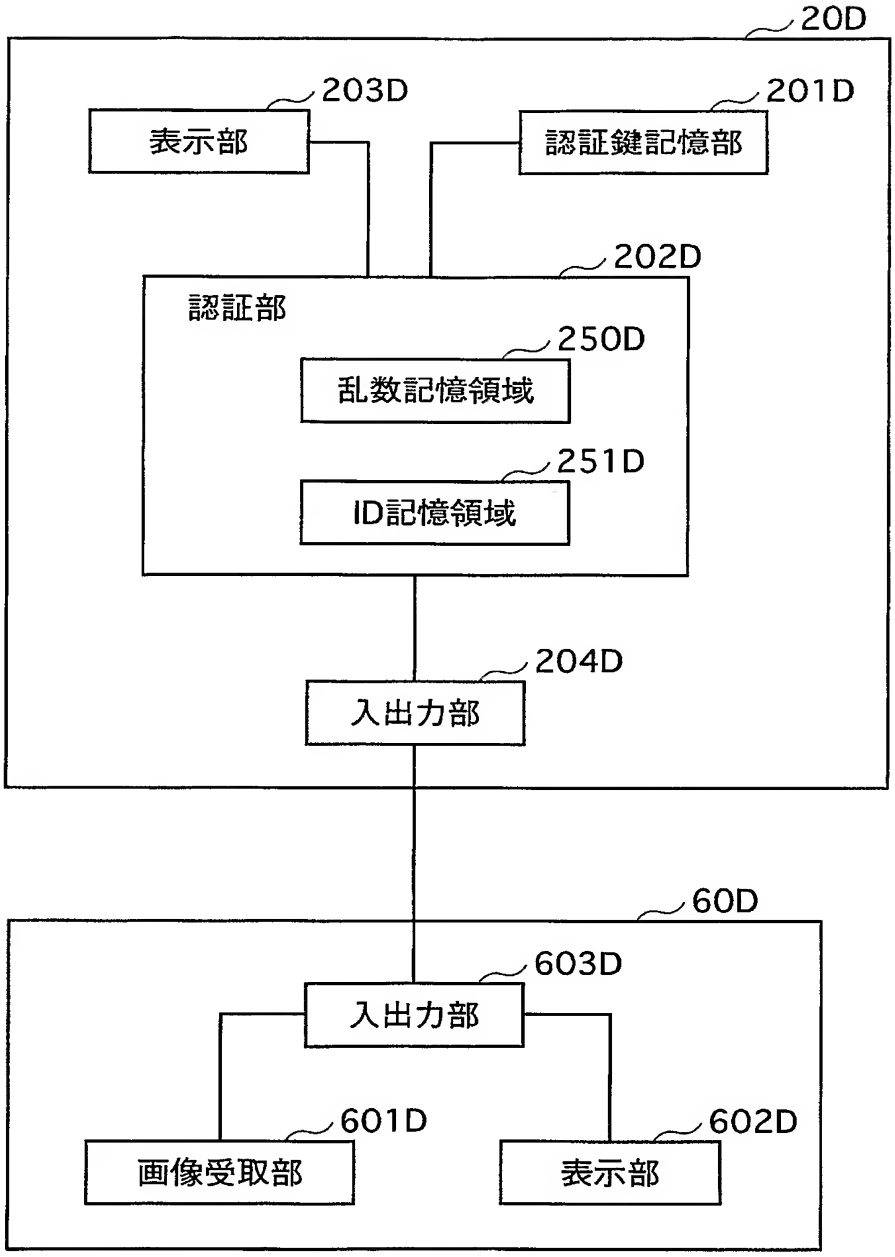
【図３０】


1D 身元認証システム
10D
11D
12D
挿入
703D
70D
702D
602D
60D
601D
40D
20D
203D
認証結果
・・・・・・です。

【図３１】


70D
703D
表示部
702D
画像受取部
カード読取部
701D
10D
103D
入出力部
102D
制御部
101D
証明鍵記憶部

【図３２】


20D
203D
表示部
201D
認証鍵記憶部
202D
認証部
250D
乱数記憶領域
251D
ID記憶領域
204D
入出力部
60D
603D
入出力部
601D
画像受取部
602D
表示部

【書類名】要約書
【要約】
【課題】　常に訪問者の身元の認証を行うことのできる認証システムを提供する。
【解決手段】　身元認証システム１は、認証カード１０、１１・・・、１２と、ユーザ端末２０と、カードリーダ３０とから構成される。
ユーザ端末２０は、カードリーダ３０に認証カード１０が挿入されると、乱数を生成し、生成した乱数を記憶するとともに、認証カード１０へ出力する。認証カード１０は、予め記憶している身元証明鍵にて受け取った乱数を暗号化して、暗号化情報を生成し、生成した暗号化情報をユーザ端末２０へ出力する。ユーザ端末２０は、受け取った暗号化情報を予め記憶している身元認証鍵を用いて復号して、復号結果を生成し、生成した復号結果と生成した乱数とが一致するか否か判断することによる認証を行う。
【選択図】　図１

特願２００３－４１０７８４

出　願　人　履　歴　情　報

識別番号　　［０００００５８２１］

１．変更年月日　　１９９０年　８月２８日
［変更理由］　　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社